ترجمة وتحرير: ممدوح الشيخ

قراءة في

الشبكات السرية

أمريكا في مواجهة أجهزة الاستخبارات الروسية والإيرانية والصينية على وسائل التواصل الاجتماعي

COVERT NETWORKS

A COMPARATIVE STUDY OF INTELLIGENCE TECHNIQUES USED BY FOREIGN INTELLIGENCE AGENCIES TO WEAPONIZE SOCIAL MEDIA

by

Sarah Ogar

December 2019

A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts



ترجمة وتحرير:

ممدوح الشيخ

قراءة في
الشبكات السرية

أمريكا في مواجهة أجهزة الاستخبارات الروسية والإيرانية والصينية على وسائل التواصل الاجتماعي

أطروحة للباحثة سارة أوجار، مقدمة إلى جامعة جونز هوبكنز وفقًا لمتطلبات الحصول على درجة الماجستير، ديسمبر 2019

الكتاب: قراءة في: الشبكات السرية
أمريكا في مواجهة أجهزة الاستخبارات الروسية والإيرانية والصينية على وسائل التواصل الاجتماعي
ترجمة وتحرير: ممدوح الشيخ
الطبعة الأولى: 2026
الناشر: المؤلف.
سلسلة: "صدقة العلم"

من الثورة البلشفية إلى تصويت خروج بريطانيا من الاتحاد الأوروبي، حاول عالم الاستخبارات السري التأثير على الأحداث العالمية بدرجات متفاوتة من النجاح.

هذا الكتاب

هذا الكتاب قراءة في أطروحة للباحثة سارة أوجار، مقدمة إلى جامعة جونز هوبكنز وفقًا لمتطلبات الحصول على درجة الماجستير، ديسمبر 2019. ومنذ العام 2016 كانت قضية الصراع الاستخباراتي على السوشيال ميديا، موضوع سيل من الكتابات في الإعلام الغربي، وبخاصة الإعلام الأمريكي.

وعندما ترجمت كتاب: "

"The Psychology of Silicon Valley, Ethical Threats and Emotional Unintelligence in the Tech Industry, Katy Cook, Springer Nature, Switzerland AG, 2020".

من الإنجليزية إلى العربية طالعت للمرة الأولى بشيئ من التفصيل قصة هذا المنعطف التاريخي في هذا الصراع الاستخباراتي الجديد، وبحسب كاتي كوك، وتحت عنوان: 2016: الانتخابات الرئاسية الأمريكية والبريكست"، فإنه، بالإضافة إلى حملات التضليل المثيرة للانقسام في جميع أنحاء العالم في البلدان التي تعتمد بشكل كبير على أخبار واتصالات فيسبوك، أُلقيت قنبلتان أخريان على الإنترنت للتطرف والمعلومات المضللة:

- الانتخابات الرئاسية الأمريكية

- قرار بريطانيا بمغادرة الاتحاد الأوروبي.

وفي الأنظمة البيئية لإنستجرام وفيسبوك ويوتيوب جوجل وتويتر، اتخذت القدرة على الإعلان عن المنتجات والرسائل للجمهور المستهدف منعطفًا مظلمًا في السنوات التي سبقت انتخابات 2016. استخدم الوكلاء الأجانب والمحليون تقنية الاستهداف الدقيق المتاحة على كل منصة للتأثير على الأنظمة السياسية في الولايات المتحدة وبريطانيا وتعطيلها، ما شجع أصوات "البريكست" في بريطانيا وانتخاب دونالد ترامب عبر البركة.

كانت شركة كيمبردج أناليتكا من أسباب أهم نجاحات الحملتين، وهي شركة لتحليل البيانات مسؤولة عن اكتناز وسرقة المعلومات المستخرجة من قاعدة مستخدمي فيسبوك المطمئنين.

وبالعودة إلى عام 2008، اكتشف باحثان من جامعة كامبريدج، هما ميشال كوسينسكي وديفيد ستيلمان، أن السلوكيات عبر الإنترنت وبيانات القياس النفسي كانت مفيدة بشكل لا يُصدَّق في التنبؤ بشخصية المستخدمين وصفاتهم وديموغرافياتهم، مثل العِرق والتوجه الجنسي والانتماء السياسي والذكاء وتعاطي المخدرات، وحتى كونهم أبناء أبوين مطلقين. وبعد بضع سنوات، في عام 2011، بدأت المتعة الحقيقية. تعاون باحث آخر من كامبريدج يدعى ألكسندر كوجان مع فيسبوك في دراسة

نُشرت في: مجلة الشخصية والاختلافات الفردية في الصداقات. وتم توفير بيانات الدراسة لكوجان بواسطة فيسبوك، وتضمنت معلومات عن 57 مليار صداقة على فيسبوك.

وبحسب الباحثة كاتي كوك، في العام نفسه، بدأ فيسبوك في تقديم ميزة على منصته تسمى: "أذونات الأصدقاء"، سمحت لمطوري الطرف الثالث بجمع كميات كبيرة من المعلومات الشخصية حول المستخدمين وأصدقائهم (بدون إذن أصدقائهم). وخلال هذا الوقت، بينما تم دمج ما يقرب من 9 ملايين تطبيق مع فيسبوك، واستُخرِجت كمية هائلة من بيانات المستخدم وحصدتها شركات مختلفة باستخدام الميزة.

وآنذاك قدر كوغان أن عشرات الآلاف من المطورين استخرجوا البيانات بالطريقة نفسها التي فعلها، وأن فيسبوك كان على دراية كبيرة بهذا الأمر، قائلاً إن الشركة اعتبرتها "ميزة وليست خطأً".

وفي عام 2013، أسس كريستوفر ويلي وألكسندر نيكس كامبريدج أناليتيكا كشركة فرعية لمجموعة SCL (مختبرات الاتصالات الاستراتيجية)، التي وصفت نفسها بأنها شركة اتصالات استراتيجية تركز على "إدارة الانتخابات العالمية". وباستخدام تقنيات معقدة لاستخراج البيانات وتحليلها، ركزت SCL بشكل أساسي

على تقديم المشورة للحكومات والمنظمات العسكرية بشأن برامج تغيير السلوك.

وفي وقت لاحق من ذلك العام، عرض نيكس وويلي قدرات كامبريدج أناليتيكا على الملياردير روبرت ميرسر، أحد مؤيدي ترامب، الذي وضع تمويلًا مبدئيًا قدره 15 مليون دولار؛ استثمر ستيف بانون، الذي أصبح فيما بعد كبير استراتيجيي ترامب، ما يقدر بنحو 1 إلى 5 ملايين دولار في الشركة.

في العام التالي، أسس كوغان وزميله جوزيف تشانسيلور شركة تدعى جلوبال سكينك ريسرش (GSR) ووقعوا عقدًا مع كيمبردج أناليتيكا لإنشاء تطبيق من شأنه أن يجمع بيانات القياس النفسي للمستخدمين على فيسبوك. بيانات كوغان وتشانسيلور المستخرجة من 270 ألف مستخدم للفيسبوك وأصدقائهم– وضمن ذلك تحديثات الحالة، والإعجابات، والرسائل الخاصة، بلغت مجموعة بيانات تضم أكثر من 87 مليون شخص.

ولاحقًا، استخدمت كيمبردج أناليتيكا بيانات كوجان وتشانسيلور لإنشاء أكثر من 30 مليون ملف تعريف مستخدم، وتحديد مجموعات الناخبين المستهدفة، وتصميم رسائل مستهدفة محددة للتأثير في آراء الناخبين وسلوكياتهم. وفي يونيو 2016، استأجرت حملة ترامب كيمبردج أناليتيكا مقابل 6 ملايين دولار وبدأت في

استخدام فيسبوك كأداة أساسية لجمع التبرعات والدعاية.

قامت الحملة بتحميل ملفات الناخبين الخاصة بها – الأسماء والعناوين وسجل التصويت وأي معلومات أخرى كانت بحوزتها عن الناخبين المحتملين – على فيسبوك. بعد ذلك ، باستخدام أداة تسمى: Lookalike Audiences، حدد فيسبوك الخصائص العامة، على سبيل المثال، الأشخاص الذين اشتركوا في رسائل ترامب الإخبارية أو اشتروا قبعات ترامب. سمح ذلك للحملة بإرسال إعلانات إلى أشخاص لديهم سمات مماثلة. وسيقوم ترامب بنشر رسائل بسيطة مثل "يتم تزوير هذه الانتخابات من قبل وسائل الإعلام التي تروج لاتهامات كاذبة لا أساس لها، وأكاذيب صريحة، من أجل انتخاب هيلاري المحدبة!" التي حصلت على مئات الآلاف من الإعجابات والتعليقات والمشاركات. وتدفقت الأموال.

وفي الوقت نفسه، لم يكن صدى رسائل كلينتون الأكثر تشويشًا على المنصة. داخل فيسبوك، أراد كل شخص تقريبًا في الفريق التنفيذي فوز كلينتون؛ لكنهم كانوا يعلمون أن ترامب كان يستخدم المنصة بشكل أفضل. إذا كان مرشح فيسبوك، وكانت مرشحة لينكد.

وفقًا لمراسلي بلومبرج، جوشوا جرين وساشا إيسنبرج، فإنه بالإضافة إلى نشر معلومات خاطئة ومثيرة للفتنة، تم

استخدام بيانات كيمبردج أناليتيكا لتشجيع قمع الناخبين: "استخدمت حملة ترامب ما يسمى بالمنشورات المظلمة – المنشورات غير العامة التي تستهدف جمهورًا معينًا – لثني الأمريكيين من أصل أفريقي عن التصويت في ولايات المعركة"

ومع ذلك ، كما يشير توفيكجي، فإن حملة ترامب "لم تكن تستخدم أداة بريئة بشكل منحرف. لقد كان يستخدم فيسبوك تمامًا كما تم تصميمه للاستخدام". لقد فعلت الحملة ذلك بثمن بخس، حيث ساعد موظفو فيسبوك، هناك في المكتب، كما تفعل شركة التكنولوجيا لمعظم المعلنين الكبار والحملات السياسية. من يهتم بمصدر الخطاب أو ما يفعله طالما يرى الناس الإعلانات؟ الباقي تم خارج فيسبوك.

بعد فوز ترامب في نوفمبر 2016، وصف زوكربيرج فكرة أن برنامجه ربما تم استخدامه للتأثير في نتائج الانتخابات الرئاسية بأنها "فكرة جميلة مجنونة!". بعد 16 شهرًا، اقتنع زوكربيرج أخيرًا. وقد أوقف فيسبوك SCL وكيبمردج أناليتيكا، وكذلك وايلي وكوجان، من المنصة. على النقيض من ذلك، تم توظيف تشانسيلور بأجر في فيسبوك منذ عام 2015.

وتبع ذلك سلسلة أحداث: إيقاف الرئيس التنفيذي نيكس من كيبمبردج أناليتيكا، إفلاس كيبمبردج أناليتيكا،

تعليق عمل 200 تطبيق من منصة فيسبوك، انخفاض سهم فيسبوك بنسبة 24٪، واعتراف الشركة بأن الأنشطة على خدمتها تشير إلى "سلوك زائف منسق" من وكالة أبحاث الإنترنت الروسية المرتبطة بالكرملين. من ناحية أخرى، تواصل شركة SCL، الشركة الأم لشركة كيمبردج أناليتيكا، الاستفادة من البيانات التي جرى الحصول عليها من فيسبوك.

وفي أوائل عام 2017، مسلحًا بالمعلومات السيكومترية لـ 230 مليون مواطن أمريكي، "فازت SCL بعقود مع وزارة الخارجية الأمريكية وكانت تتجه إلى البنتاغون". في الوقت نفسه تقريبًا، كان المواطنون البريطانيون يتعاملون مع كابوس انتخابي خاص بهم. وفي جلسة أمام اللجنة الرقمية والثقافة والإعلام والرياضة، أوضح ويلي لأعضاء البرلمان كيف أن التصويت في استفتاء الخروج من الاتحاد الأوروبي "تم الفوز به من خلال الاحتيال" عبر حملة التصويت للخروج "بتوجيه الأموال بشكل غير صحيح من خلال شركة تقنية لها روابط مع كيبمبرج أناليتيكا".

قال ويلي إنه كان من اللافت للنظر أن التصويت للخروج و3 مجموعات أخرى مؤيدة لخروج بريطانيا من الاتحاد الأوروبي استهدفت الطلاب. وقدامى المحاربين من أجل بريطانيا والحزب الاتحادي الديمقراطي في أيرلندا الشمالية – استخدموا جميعًا خدمات الشركة غير

المعروفة Aggregate IQ (AIQ) للمساعدة في استهداف الناخبين عبر الإنترنت. وأخبر أعضاء البرلمان أن AIQ كانت فعليًا الذراع الكندية لشركة كيمبردج أناليتيكا، حيث تستمد معظم دخلها من خلال العمل كمقاول فرعي.

ويخضع خلط الأموال بين حملتي "التصويت للخروج" و"BeLeave"، التي أُنفِقَت على خدمات AIQ، حاليًا للتحقيق من قبل لجنة الانتخابات في بريطانيا. وقد فاز استفتاء الاتحاد الأوروبي بهامش ضئيل (2٪) من الأصوات، وهي نتيجة يعتقد ويلي أنها كانت ستختلف تمامًا لولا مشاركة AIQ، جنبًا إلى جنب مع الانتهاك المحتمل لحدود الإنفاق على الحملة.

ويلي، الذي كان يبلغ من العمر 24 عامًا فقط عندما ساعد نيكس في تشكيل كيمبردج أناليتيكا، يصف الشركة الآن بأنها "آلة دعاية كاملة الخدمات". وقد أخبرت كارول كادوالادر، مراسلة الغارديان التي فجرت الفضيحة، أنه يعتقد أن الأساليب التي استخدمتها كامبريدج أناليتيكا والحملات التي وظفتها كانت "أسوأ من التنمر. لأن الناس لا يعرفون بالضرورة أن ذلك يحدث لهم".

وبشكل أساسي، فإن حرب المعلومات لا تفضي إلى الديمقراطية. وأهمية المعلومات الصحيحة والدقيقة أمر ضروري لمؤسسة الديمقراطية. القاضية الأمريكية إيمي بيرمان جاكسون، التي حكمت على مدير حملة ترامب بول

مانافورت في عام 2019 بتهم متعددة، ضمنها الاحتيال الضريبي والتآمر، قالت في الحكم، إنه إذا "لم يكن لدى الناس الحقائق، فلن تنجح الديمقراطية". وفي مقال لمجلة بوسطن ريفيو، تصف كلارا هندريكسون على وجه التحديد أولويات فيسبوك وإنستغرام بأنها متناقضة مع الديمقراطية، مشيرة إلى أن سياساتها "أثبتت أنها تفكك الديمقراطية الليبرالية وتستقطبها وتهددها".

ووفقًا لتقرير الديمقراطية السنوي لعام 2018 الصادر عن جامعة جوتنبرج، بدأت الديمقراطية بالتراجع في عامي 2006 و2007 عبر عدد من المناطق، وضمن ذلك أمريكا اللاتينية ومنطقة البحر الكاريبي وأوروبا الشرقية وأمريكا الوسطى والشرق الأوسط وشمال إفريقيا وأوروبا الغربية وأمريكا الشمالية.

وهذه السنوات، من قبيل الصدفة، تعتبر أساسية في التكنولوجيا. كان عام 2006 هو العام الذي تم فيه إطلاق تويتر، وتم إطلاق فيسبوك للجمهور، واستحوذت جوجل على يوتيوب. وفي يونيو من العام التالي، ظهر آي. فون لأول مرة. وقد كانت المنطقتان الوحيدتان اللتان وجد التقرير أن الديمقراطيات فيهما تتحسن بدلاً من التراجع هما أفريقيا جنوب الصحراء الكبرى وآسيا، التي، وفقًا لتحليل التقرير، المنطقتان الوحيدتان اللتان تقل معدلات انتشار الإنترنت فيهما عن المتوسط العالمي (بعبارة

أخرى، هاتان المنطقتان لا تستخدمان الإنترنت بقدر ما تستخدمهما تلك التي تشهد ديمقراطياتها الانحدار).

وبالإضافة إلى التلاعب الداخلي بالانتخابات الأمريكية والبريطانية، لعب التأثير الأجنبي على وسائل التواصل الاجتماعي أيضًا دورًا مهمًا، لا سيما التدخل الروسي. في إحدى جلسات الاستماع في الكونغرس لعام 2018، اعترف موقع فيسبوك بأنه تم العثور على 170 حسابًا على و120 صفحة على تويتر قد نشرت دعاية من وكالة أبحاث الإنترنت الروسية.

وإذا كان الرقم 120 لا يبدو سيئًا للغاية، فتأمل حقيقة أنه تمت مشاركة منشورات من 6 فقط من الحسابات الروسية التي تم تعليقها بواسطة فيسبوك عددًا هائلاً 340 مليون مرة. والتحقيقات في انتصار ترامب، وخروج بريطانيا من الاتحاد الأوروبي، والتدخل الروسي جارية حاليًا في وقت كتابة هذا التقرير، وبمجرد اكتمالها، من المرجح أن توضح واحدة من أكثر الهجمات شمولاً وتدميرًا، ولا يمكن تصورها على الديمقراطية في التاريخ الحديث.

روسيا، فيسبوك، ترامب، ميرسر، بانون، بريكست. كل واحد من هذه الخيوط يمر عبر كيمبردج أناليتيكا. حتى في الأسابيع القليلة الماضية، يبدو أن فهم دور فيسبوك قد توسَّع وتعمَّق. كانت لوائح اتهام مولر جزءًا من ذلك، لكن

بول أوليفييه ديهاي، خبير بيانات وأكاديمي مقيم في سويسرا، نشر بعض الأبحاث الأولى في عمليات كيمبردج أناليتيكا – يقول إنه أصبح واضحًا بشكل متزايد أن فيسبوك "مسيء بحسب التصميم". وإذا كان هناك دليل على تواطؤ بين حملة ترامب وروسيا، فسيكون في تدفقات البيانات من المنصة.

الآلية التي تم بها "اختطاف فيسبوك، وإعادة توجيهه ليصبح مسرحًا للحرب"، و"كيف أصبح منصة انطلاق لما يبدو أنه هجوم استثنائي على العملية الديمقراطية في الولايات المتحدة"، مخيف ومعقد في الوقت نفسه. ومع ذلك، فإن الدافع الذي سمح لها بالاستمرار أكثر وضوحًا: الإيرادات الناتجة عن الإعلانات.

....

وهذا الكتاب هو ببساطة قراءة في رسالة الماجستير المشار إليها، وقد حرصت على ألا يتشتت القاريء بإغراقه في سيل من المعلومات والتحليلات التي تستعصي على الحصر، منذ الانتخابات الرئاسية الأمريكية 2016.

ومحتوى الرسالة كان موضوع عدة حلقات على قناتي على يوتيوب

- بتوقيع ممدوح الشيخ
- رواق ممدوح الشيخ

وهذا الكتاب جزء من مسعى لإشاعة العلم على أوسع نطاق في إطار: "صدقة العلم".
وأسأل الله أن يتقبله وأن ينفع به.

ممدوح الشيخ
القاهرة
22 مايو 2026

تقديم

في عام 2016، كان أحد أكثر مظاهر عمليات الاستخبارات الروسية وقاحة موجهًا ضد ملايين الأمريكيين عندما صوتوا لانتخاب رئيس جدي. ورغم أن هذه لم تكن المرة الأولى التي تحاول فيها روسيا التأثير في الانتخابات الرئاسية الأمريكية، إلا أنها كانت بلا شك أكبر محاولة من حيث نطاقها والأكثر شهرة حتى الآن.

رغم كثرة النقاشات التي أعقبت انتخابات عام 2016، إلا أنه لم يكن هناك الكثير من التحليلات التاريخية المنسقة التي تضع أحداث عام 2016 في سياقها التاريخي. وظهور وسائل التواصل الاجتماعي غيّر عملية جمع المعلومات الاستخباراتية من حيث شكلها، لكن ليس من حيث جوهرها.

باستخدام أسلوب دراسة الحالة، توضح الأطروحة كيف تطبق 3 دول مختلفة تقنيات الاستخبارات الكلاسيكية على البيئة الحديثة لوسائل التواصل الاجتماعي.

الصين استخدمت أساليب تجنيد العملاء الكلاسيكية من خلال مواقع مثل لينكد إن، واستخدمت إيران أساليب الإيقاع التقليدية عبر مزيج من مواقع التواصل الاجتماعي، ووظفت روسيا التكتيكات الكلاسيكية للابتزاز والتزوير وعملاء النفوذ والجماعات الواجهة في حملات التأثير السرية الحديثة.

كيفن إي. كروس،
مايكل إس. سميث الثاني

مقدمة

في عام 2016، أفادت وكالات الاستخبارات الأمريكية أن أجهزة الاستخبارات الروسية حاولت التأثير في الانتخابات الرئاسية لعام 2016 من خلال استهداف ملايين الأمريكيين عبر حملة تضليل على منصات التواصل الاجتماعي المتعددة. كان تحويل منصات التواصل الاجتماعي الشهيرة مثل: فيسبوك وتويتر إلى أدوات تُستخدم لشن حملة تدخل في الانتخابات ضد الولايات المتحدة استراتيجية جديدة من بعض النواحي.

ومع ذلك، فإن التحليل المقارن الشامل لحملة التدخل في الانتخابات هذه وعمليات التأثير السرية للاتحاد السوفيتي خلال الحرب الباردة يشير إلى أن المخابرات الروسية قامت، ببساطة، بتكييف النموذج السوفيتي لشن حملات تأثير خبيثة.

وفي الوقت نفسه، ليست روسيا الدولة الوحيدة التي استخدمت وسائل التواصل الاجتماعي للتلاعب بسكان أجانب. ومؤخرًا نُسبت إلى أجهزة المخابرات

الإيرانية والصينية محاولات ملحوظة لاستخدام منصات التواصل الاجتماعي الشهيرة لشن عمليات تأثير سرية.

وبما أن هؤلاء الفاعلين ينظرون بوضوح إلى منصات التواصل الاجتماعي الشهيرة كأدوات جذابة يمكن استخدامها لشن عمليات التأثير، فمن الضروري النظر في طرق بناء القدرة على الصمود في وجه هذه الأنشطة.

إن تحسين الفهم الحالي لكيفية استخدام وسائل التواصل الاجتماعي من قبل هذه الجهات الفاعلة وغيرها لتحديث عمليات الاستخبارات التقليدية بين الحكومات والقطاع الخاص والسكان المدنيين يمكن أن يساعد في تحقيق هذا الهدف.

تهدف هذه الأطروحة إلى الإجابة على سؤال:

ما أساليب الاستخبارات الكلاسيكية التي تفضلها وكالات الاستخبارات الأجنبية المحددة عندما تستخدم وسائل التواصل الاجتماعي كسلاح. ولتحقيق هذا الهدف، قام المؤلف بتحليل لدراسات الحالة لعمليات الاستخبارات الخارجية التي نفذتها روسيا وإيران والصين.

يتناول قسم جهود روسيا للتدخل في الانتخابات الرئاسية الأمريكية لعام 2016 كيفية استخدام أجهزة المخابرات الروسية لتقنيات استخباراتية معروفة كانت يستخدمها في السابق الاتحاد السوفيتي. ويتناول قسم أنشطة النظام الإيراني في المجال الإلكتروني حملات التأثير

السرية عبر الإنترنت التي تتوسع باطراد، ما يشير إلى أن أجهزة المخابرات الإيرانية تفضل استخدام الفخاخ الرقمية. ويتناول قسم عمليات الاستخبارات الصينية عبر الإنترنت كيفية تطوير الجواسيس الصينيين لخبرة في توليد تعريفات شخصية عبر الإنترنت أدت إلى تجنيد عملاء ناجحين.

وفي الوقت نفسه، تكشف الأطروحة كيف تستغل وكالات الاستخبارات الأجنبية التغيرات الاجتماعية الناجمة عن البيئة الرقمية، ووسائل التواصل الاجتماعي على وجه الخصوص، لتوسيع قدراتها على شن عمليات تأثير واسعة النطاق، فضلًا عن تجنيد أصول جديدة.

منذ ظهورها، أصبحت وسائل التواصل الاجتماعي جزءًا لا يتجزأ من التفاعل الشخصي المعاصر. ورغم أن العديد من الباحثين قد استكشفوا التأثيرات العامة لهذه الوسائل على التواصل بين الأشخاص، إلا أن قلة من الباحثين تناولوا أسئلة حول كيفية تأثير وسائل التواصل الاجتماعي على مجال جمع المعلومات الاستخباراتية.

وقد استخدمت وكالات الاستخبارات الأجنبية وكيانات الاستخبارات الأجنبية، وتشمل أيضًا الجماعات الإرهابية الدولية وسائل التواصل الاجتماعي وغيرها من الأدوات الرقمية للوصول إلى الشركات والحكومات والأفراد.

وكما أوضحت حملة التأثير الروسية سيئة السمعة في عام 2016، فإن وسائل التواصل الاجتماعي تسمح للمؤسسات الأجنبية بالوصول المباشر إلى شريحة أكبر من عامة السكان في الولايات المتحدة مقارنة بما كانت قادرة على التفاعل معه خلال القرن العشرين.

لاحظ مكتب مدير الاستخبارات الوطنية (ODNI) في استراتيجيته الوطنية للاستخبارات لعام 2019 ما يلي:

تتيح التطورات التكنولوجية السريعة لمجموعة واسعة من المؤسسات الأجنبية نشر قدرات متطورة بشكل متزايد واستهداف الحكومة وشركاء القطاع الخاص والأوساط الأكاديمية بقوة.

تتسم الشركات الأجنبية ذات المصالح الخاصة بالاستباقية وتستخدم أساليب إبداعية – وضمن ذلك استخدام الأدوات الإلكترونية، والجواسيس الداخليين، والتجسس، واستغلال سلسلة التوريد - لتعزيز مصالحها واكتساب ميزة على الولايات المتحدة. وتؤدي هذه الأنشطة إلى تفاقم التهديدات التقليدية التي تواجهها مؤسسات إنفاذ القانون الفيدرالية.

الشركات الخاصة العاملة في قطاع أمن تكنولوجيا المعلومات تتفق مع تقييم مكتب مدير الاستخبارات الوطنية بشأن تسليح وكالات الاستخبارات الأجنبية

لوسائل التواصل الاجتماعي والاعتماد المتزايد على الأدوات الإلكترونية.

وقد خلصت شركة الأمن السيبراني FireEye إلى أن "الدول في جميع أنحاء العالم تولي أهمية قصوى لتحسين قدراتها السيبرانية"، وغالبًا تشمل الاستفادة من الشبكات الاجتماعية للمجرمين الإلكترونيين واستخدام الأدوات السيبرانية المتاحة تجاريًا.

في إشارة إلى برنامج إيران السيبراني المتنامي، حثت شركة الأمن السيبراني F-Secure المؤسسات الإعلامية والمنصات على "النظر في المخاطر المحددة التي تشكلها الجهات الحكومية المتورطة في الهجمات السيبرانية وإساءة استخدام وظائف المنتج الأصلية".

وقد خلصت شركة فاير آي مؤخرًا إلى أن إيران أنشأت شبكة من الشخصيات المزيفة على وسائل التواصل الاجتماعي والتي "انتحلت شخصيات المرشحين السياسيين الجمهوريين الذين ترشحوا لمقاعد مجلس النواب في انتخابات التجديد النصفي للكونغرس الأمريكي لعام 2018".

في مارس 2019، أصدرت شركة Recorded Future المتخصصة في استخبارات التهديدات السيبرانية تقريرًا حلَّل البيانات من مختلف منصات التواصل الاجتماعي الغربية من أكتوبر 2018 حتى فبراير 2019 لتقييم الطرق

التي تستغل بها الصين وسائل التواصل الاجتماعي للتأثير في الرأي العام الأمريكي. وخلص باحثو الشركة إلى أن أساليب التأثير السري الصينية تختلف اختلافًا كبيرًا عن تلك التي تستخدمها روسيا.

وبعبارة أخرى، بينما يقوم عملاء التأثير السري الروس بمهاجمة الخصوم بقوة وإبعادهم عنهم عبر وسائل التواصل الاجتماعي، فإن شخصيات التأثير السري الصينية "تقدم صورة إيجابية وحميدة وتعاونية للصين" وتختار نهجًا أكثر ليونة ودبلوماسية من أجل تحقيق أهداف السياسة الخارجية الصينية المحددة.

في القطاع العام، تتواصل مختلف الوكالات الحكومية مع كيانات القطاع الخاص من أجل تطوير فهم استراتيجي جماعي للخصم الذي يقف وراء هذه التهديدات. وفي عام 2017، أنشأ مكتب التحقيقات الفيدرالي مكتب القطاع الخاص الذي يسعى إلى التواصل بشكل استباقي مع مالكي البنية التحتية المملوكة للقطاع الخاص في أمريكا ومعالجة التهديدات الناجمة عن هذه البنية التحتية المملوكة للقطاع الخاص.

في مؤتمر عقد عام 2019، سلط مدير مكتب التحقيقات الفيدرالي كريستوفر راي الضوء على كيف يمكن أن يكون انخراط القطاعين العام والخاص في مواجهة التهديدات الإلكترونية مفيدًا للطرفين، مستشهدًا

بجهود مكتب التحقيقات الفيدرالي للتواصل مع مزودي وسائل التواصل الاجتماعي قبل انتخابات التجديد النصفي لعام 2018.

كما وجهت القيادة السيبرانية دعوات عامة للمشاركة في مواجهة التهديد السيبراني الذي يهدد المواطنين الأمريكيين والبنية التحتية.

في ديسمبر 2017، أعلنت جانيت مانفرا، مساعدة وزير الأمن السيبراني والاتصالات في وزارة الأمن الداخلي، أن وزارة الأمن الداخلي تسعى إلى "تجاوز مجرد تقديم المساعدة الطوعية" للقطاع الخاص الأمريكي من خلال زيادة استخدام مذكرات التفاهم الاستباقية قبل وقوع التهديدات السيبرانية للأمن العام.

ترى شركة الأمن السيبراني FireEye أنه بغض النظر عن النشاط السيبراني الخبيث، فإن "فهم الخصم هو المفتاح للحماية من الهجمات، فرغم أنه لا يمكنك التنبؤ بجميع الهجمات، إلا أنه يمكنك على الأقل استخدام المعلومات الاستخباراتية من الماضي لإبلاغ الهجمات المستقبلية المحتملة والمساعدة في تخفيف العواقب."

يُعدّ استهلاك معلومات الخصوم أمرًا بالغ الأهمية للمؤسسات، فمن أجل حماية نفسك، تحتاج إلى معرفة من سيلاحقك وكيف سيلاحقك.

وورد في تقرير مكتب مدير الاستخبارات الوطنية تحت عنوان: "الأولوية القصوى لمهمة الاستخبارات الأمريكية":

تتمثل مهمة المجتمع في جمع "المعلومات الاستخباراتية الاستراتيجية" أو بعبارة أخرى، جمع المعلومات الاستخباراتية التي "تتناول قضايا ذات أهمية دائمة للأمن القومي". وكما توضح الأمثلة المذكورة أعلاه، فإن استخدام وكالات الاستخبارات الأجنبية لوسائل التواصل الاجتماعي وغيرها من الأدوات الرقمية كسلاح يظل مصلحة دائمة للأمن القومي.

لذا، فإن من الأهمية بمكان أن يستكشف الباحثون الأكاديميون الاستراتيجيات الكلاسيكية التي يُعاد استخدامها في عمليات الاستخبارات التي تجري في وسائل التواصل الاجتماعي.

إذا أفلتت الاستراتيجيات المتأثرة بالأساليب الكلاسيكية التي تقف وراء عمليات الاستخبارات على وسائل التواصل الاجتماعي من الفحص، فمن المرجح ألا تحدث أية تغييرات في الهياكل الأمنية داخل وسائل التواصل الاجتماعي.

ومن الأمور المبشرة أن تحاول الحكومة الأمريكية أن تكون استباقية في تواصلها مع الشركات الخاصة، لكن ينبغي أن يشمل جزء من ذلك تقديم معلومات

استخباراتية تمهيدية بشأن آليات عمل الخصم وتراثه الثقافي. وبدون فهم تاريخي لكيفية استهداف أجهزة الاستخبارات الأجنبية للمواطنين، من المرجح أن يظل النقاش العام مركزًا على الجوانب التقنية لمنصات التواصل الاجتماعي نفسها وليس على الدوافع والتكتيكات الكامنة التي دفعت أجهزة الاستخبارات الأجنبية اليوم إلى استهداف المواطنين الرقميين داخل مجال التواصل الاجتماعي.

يُتيح موضوع عمليات الاستخبارات الأجنبية في وسائل التواصل الاجتماعي للباحثين فرصة إدخال الخبرات التاريخية لمحترفي الاستخبارات في النقاش العام الأوسع. وحتى الآن، ركزت معظم المعلومات المتاحة حول عمليات الاستخبارات في وسائل التواصل الاجتماعي فقط على آثارها المباشرة وكذلك ردود الفعل العاطفية تجاهها، بدلًا من التركيز على التاريخ.

وهدف الدراسة الإجابة على سؤال كيفية تطبيق وكالات الاستخبارات الأجنبية الحديثة تقنيات الاستخبارات الكلاسيكية على المجال الحديث لوسائل التواصل الاجتماعي. وستمنح القارئ رؤية للتأثيرات التاريخية على الاستراتيجيات المستخدمة حاليًا للتأثير في القيم والتصورات والمعتقدات الأمريكية.

وعمليات الاستخباراتية غالبًا تسفر عن روايات مقنعة، وهي في نهاية المطاف سلسلة من العمليات المترابطة. وفيما يتعلق باختيار الدول التي سيتم دراستها، تم اختيار هذه الدول بناءً على كمية المعلومات المتاحة للجمهور، وأهمية الدولة المعادية للسياسة الخارجية الأمريكية، وتصنيف الدولة المستمر كأولوية استخباراتية أمريكية.

رغم أن العديد من الدول تجمع معلومات استخباراتية عن الولايات المتحدة، فإن الدول المعادية مثل: روسيا وإيران والصين لا تمتلك النية فحسب، بل تمتلك أيضًا القدرة المؤكدة على تنفيذ حملات استخباراتية خارجية متطورة عبر وسائل التواصل الاجتماعي.

نظرًا للطبيعة السرية للعديد من الأنشطة الاستخباراتية، هناك العديد من العوائق التي تحول دون إجراء دراسات حول العمليات الاستخباراتية بالنسبة لعلماء الدراسات الأمنية الذين يقومون بأبحاث غير مصنفة.

وبينما هناك عوائق عديدة عندما يتعلق الأمر بالوصول العام إلى المعلومات الاستخباراتية السرية، فإن أحد أنواع المعلومات الاستخباراتية التي ينبغي ذكرها عند

تناول العمليات الاستخباراتية في وسائل التواصل الاجتماعي هو: "مفهوم الاستخبارات مفتوحة المصدر".

وعند استخدام المصطلح في مجتمع الاستخبارات، فإنه يعني مجموعة معلومات متاحة للجمهور ويجري جمعها وتحليلها للمساهمة في منتجات الاستخبارات النهائية. وكان "مفهوم الاستخبارات المفتوحة" مجموعة فرعية معترفًا بها من الاستخبارات لفترة، لكن مؤخرًا، خضع لعدة تغييرات، معظمها يتعلق بتوسيع البيانات المتاحة للجمهور والحاجة اللاحقة إلى تعريف أكثر دقة لهذه الممارسة الاستخباراتية.

مع توسع مصادر البيانات المتاحة للجمهور، افترض باحثون أن المنهجيات الكامنة وراء جمع المعلومات الاستخباراتية مفتوحة المصدر تتطلب تحسينًا. ويندرج جمع المعلومات المتاحة من وسائل التواصل الاجتماعي ضمن التعريف الواسع للاستخبارات مفتوحة المصدر. ويمكن الحديث مطولًا عن تعقيدات البحث في المصادر المفتوحة وكيف غيّر ممارسات جمع المعلومات الاستخباراتية.

خارج نطاق الاستخبارات مفتوحة المصدر، لا تزال معظم المعلومات الاستخباراتية محصورة ومحجوبة عن الباحثين الأكاديميين. ولدراسة هذا الموضوع، يعتمد معظم باحثي الاستخبارات على منهج تاريخي أو ثقافي.

باحثون مثل مايكل وارنر ومارك فيثيان وكريستوفر أندرو أنتجوا نظرة عامة شاملة على أجهزة الاستخبارات بأكملها باستخدام هذه الأساليب. منحت بعض وكالات الاستخبارات، مثل جهاز MI-5 البريطاني، وصولًا غير مقيد على ما يبدو إلى أرشيفاتها. وفي حالات أخرى، يتخذ البحث الأرشيفي شكل تشريح لأنظمة الاستخبارات المنهارة. كاثرين فيرديري في بحثها الإثنوغرافي حول جهاز الأمن الروماني السابق سقوط الدولة الأمنية التي يديرها الاتحاد السوفيتي في رومانيا، لم تكشف فقط عن المعلومات الاستخباراتية التي جمعها جهاز الأمن عنها، بل كشفت أيضًا عن الملفات التي كشفت عن العمليات الداخلية والعلاقات الاجتماعية لجهاز المخابرات الروماني.

وبعيدًا عن الوصول المشروع إلى أرشيفات الاستخبارات، هناك أيضًا حالات أدى فيها الوصول غير المشروع إلى زيادة المعرفة الثقافية والوعي لدى الجمهور بكيفية عمل وكالات الاستخبارات. ورغم اختلاف المنشقين في درجات وصولهم وموثوقيتهم، إلا أنه لا يمكن إنكار أن باحثي الاستخبارات يستفيدون بشكل كبير من الروايات المباشرة للمنشقين الأجانب.

شخصيات مثل فاسيلي ميتروخين وليتفينينكو وسيرجي تريتياكوف نشروا أرشيفات قيّمة من المعلومات السرية التي أفادت الباحثين، ما أدى في بعض الأحيان إلى

اكتشاف شبكات تجسس واسعة النطاق كما كان الحال مع مساعدة تريتياكوف في طرد المهاجرين غير الشرعيين الروس.

أحد المناهج متعددة التخصصات في مجال الاستخبارات التي استخدمها بعض الباحثين: دراسة علم نفس التجسس وكيف تغير هذا العلم من عالم ما قبل وسائل التواصل الاجتماعي إلى عالم ما بعد وسائل التواصل الاجتماعي. واستخدم باحثون آخرون نهج البحث السيبراني لدراسة الطرق الواسعة التي تلعب بها التكنولوجيا دورًا في جمع المعلومات الاستخباراتية. بالإضافة إلى ذلك، بدأ باحثون في مجال التكنولوجيا في تركيز جهودهم على وسائل التواصل الاجتماعي على وجه الخصوص وعلى الجوانب القانونية لدورها كمنصة لجمع المعلومات الاستخباراتية الخارجية.

ودخلت دراسة الأخلاقيات في مجال الاستخبارات، وبخاصة أخلاقيات جمع المعلومات الاستخباراتية عبر وسائل التواصل الاجتماعي وإمكانية تنظيمها، في النقاش في أدبيات الدراسات الاستخباراتية الأمريكية. ومع ذلك، فبينما تكتشف دول أخرى ما تعتقد أنه تدخل في انتخاباتها وشؤونها الداخلية الأخرى، تتزايد المنشورات الدولية لأبحاث الاستخبارات التي تركز على وسائل التواصل الاجتماعي ضمن هذا المجال من الدراسة.

الآن وقد قام جواسيس عديدون بنقل اتصالاتهم السرية من الخطوط الأرضية الآمنة إلى تطبيقات المراسلة المشفرة، فمن المهم دراسة أية جوانب من أساليب العمل التقليدية تفيد ممارسي الاستخبارات اليوم.

ورغم أن العديد من الأمريكيين يدركون الآن أن روسيا ودول أخرى تجمع كميات هائلة من المعلومات باستخدام المصادر والأساليب عبر الإنترنت، إلا أن ما تفعله وكالات الاستخبارات الأجنبية بهذه المعلومات تحديدًا وكيف تستخدم تقنيات الاستهداف البشري التقليدية هي مواضيع تستدعي مزيدًا من النقاش.

منعطف الانتخابات الأمريكية

في أواخر عام 2016، حاول مجلس الشيوخ الأمريكي فهم سلسلة من الأحداث التي بدت مترابطة ومثيرة للقلق للغاية، وبدت مرتبطة بعملية استخبارات رقمية منسقة استهدفت الانتخابات الرئاسية. في سعيها للحصول على إجابات نيابة عن الشعب الأمريكي، لم يكتفِ الكونغرس بالاستعانة بأكبر 3 وكالات استخبارات في أمريكا، بل استدعى أيضًا مزودي وسائل التواصل الاجتماعي في أمريكا، حيث استدعي رؤساءهم التنفيذيون للإدلاء بشهادتهم في جلسات استماع الكونغرس.

من المشكوك فيه أن يكون زوكربيرج على دراية بجميع التداعيات التي ستنتج عن الشبكة الاجتماعية التي أنشأها في غرفة سكنه الجامعي في أوائل العقد الأول من القرن 21، لكن لا شك في أنه عقب انتخابات 2016 الرئاسية، واجه زوكربيرج والأمريكيون العديد من الحقائق القاسية حول وسائل التواصل الاجتماعي.

والأهم من ذلك، أن الأمريكيين واجهوا حقيقة مزدوجة مفادها أنه، بينما، وسائل التواصل الاجتماعي لديها القدرة على جمع جميع مواطني العالم معًا، فإن "العالم الحقيقي" يشمل جميع إرهابيين وخونة وجواسيس.

قبل انتخابات عام 2016، كان هناك القليل جدًا من الأبحاث التي تناولت الواقع المزدوج لوسائل التواصل الاجتماعي أو حتى إمكانية استخدام أجهزة الاستخبارات المعادية لوسائل التواصل الاجتماعي كسلاح. وبالنظر إلى العدد المتزايد من العمليات السرية التي تُجرى على وسائل التواصل الاجتماعي والنقاش العام غير المثمر نسبيًا، فمن الواضح أن صانعي السياسات والمواطنين والأكاديميين ما زالوا يفتقرون إلى الوضوح في بعض المجالات، لا سيما في الجوانب التقنية لهذه العمليات.

بصرف النظر عن الجوانب التقنية، فإن تاريخ أجهزة الاستخبارات الأجنبية وحملاتها السابقة ضد

المصالح الأمريكية أمر غالبًا ما يتم التغاضي عنه أو تناوله في جملة أو جملتين. وجرى تسليط الضوء على هذه القضية في رد الكونغرس في يوليو 2018 على تقييم مجتمع الاستخبارات لعام 2017. رغم أن الكونغرس بدا أنه يقدر ويثمن الجهود المشتركة لمجتمع الاستخبارات الأمريكي، إلا أن الكونغرس لاحظ أن الروايات التاريخية والمصطلحات واللغة التي استندت إليها العمليات الاستخباراتية لعام 2016 كانت غائبة بشكل ملحوظ عن تقييم مجتمع الاستخبارات لعام 2017.

ونظرًا للاهتمام المستمر بالسياق التاريخي لعمليات الاستخبارات، فمن المهم أن تسلط الأبحاث المستقبلية في عمليات الاستخبارات في وسائل التواصل الاجتماعي الضوء على طول عمر واستمرارية الاستخبارات من خلال المقارنات التاريخية.

الفصل الأول
الاستخبارات الروسية في وسائل التواصل الاجتماعي

في عام 2015، صرّح السفير الأمريكي لدى ألمانيا بأن آلة التضليل الروسية عبارة عن حملة إعلامية بقيمة 400 مليون دولار في أكثر من 100 دولة، وبعد عام واحد، واجه المواطنون الأمريكيون حقيقة هذا التصريح المُرّة عندما بدا أن روسيا تحاول التأثير على الانتخابات الرئاسية الأمريكية لعام 2016.

بدأت القصة بتقارير تفيد باختراق خادم تابع للمؤتمر الوطني الديمقراطي. وبعد أيام من الاختراق، نُشرت وثائق كثيرة من خادم المؤتمر على الإنترنت. وبعد ذلك بوقت قصير، بدأت تظهر حسابات ومجموعات وهمية على مواقع التواصل الاجتماعي المختلفة، وكأنها ظهرت فجأة من العدم.

بدا أن الرابط المشترك بين كل هذه الأنشطة هو خصم أمريكا في الحرب الباردة: روسيا. لكن ما لم يُناقش في أعقاب هذه الأنشطة مباشرةً هو ما إذا كان هذا النوع من التأثير الخبيث حدث سابقًا. ويكشف فحص تاريخ الاستخبارات الروسية أن ما حدث عام 2016 لم يكن المرة الأولى التي توجه فيها روسيا مواردها الاستخباراتية ضد الانتخابات الرئاسية الأمريكية. وقد استخدمت روسيا المنهج نفسه وأساليب التدابير الفعالة نفسها ضد الانتخابات الرئاسية في الحرب الباردة وفي عام 2016.

ومع ذلك، فإن ظهور الأدوات السيبرانية قد خلق المزيد من سبل التنفيذ وعزز أنشطة النفوذ الروسي الأخيرة في عام 2016. وفي كلتا الحالتين، سعت روسيا إلى تشويه سمعة مرشح رئاسي أمريكي على حساب آخر واستغلال الانقسامات الاجتماعية والسياسية الداخلية في الولايات المتحدة. وبعيدًا عن أهدافها التكتيكية، استخدمت روسيا العديد من الأساليب الشائعة في الحرب الباردة في عام 2016.

ورغم أن روسيا تستخدم مجموعة واسعة من أساليب التأثير السرية، إلا أن هناك العديد منها التي تم تحديدها وتقييمها على أنها الأكثر أهمية لجهاز المخابرات الروسي.

تُعد هذه الأساليب جزءًا مما تسميه روسيا "التدابير الفعالة"، وتشمل:

- جماعات الواجهة.
- عملاء النفوذ.
- الابتزاز.
- التزوير.

يُعد تحليل هذه الأساليب الاستخباراتية التاريخية أمرًا بالغ الأهمية إذا لم يرغب خبراء الاستخبارات الأمريكيون في تكرار أخطاء الماضي. ولهذا السبب، سيجري هذا الفصل مقارنة نقدية بين آليات التأثير السري التاريخية والحديثة لروسيا.

المصادر التاريخية والمتعددة التخصصات يمكنها المساعدة بشكل كبير في تحليل أية ظاهرة سياسية. وتُعدّ "التدابير الفعّالة" موضوعًا تناوله المؤرخون والباحثون الحكوميون وخبراء الأمن السيبراني، وربما الأهم من ذلك، العاملون في مجال الاستخبارات الروسية أنفسهم.

تاريخ التدابير الفعالة

المصطلح الروسي: "الإجراءات الفعالة" ليس له مقابل مباشر في اللغة الإنجليزية. وحاولت مصطلحات طبية مثل: "الحرب النفسية" ومصطلحات عامية مثل: "الحيل القذرة" استيعاب بعض معانيها، لكن لا توجد

كلمة إنجليزية واحدة تصف: "التدابير الفعالة" بشكل كافٍ ضمن معجم الاستخبارات الغربية.

ويقدم كتاب: "استراتيجية التضليل السوفيتي" أحد أكثر التعريفات إيجازًا، حيث يصف التدابير الفعالة بأنها "مجموعة أساليب علنية وسرية للتأثير في الأحداث والسلوكيات في الدول الأجنبية". وقدم المنشق السوفيتي فاسيلي ميتروخين تعريفًا أكثر تفصيلًا، حيث يعرفها في كتابه: "معجم الكي. جي. بي." بأنها: "تدابير عملياتية تهدف إلى ممارسة تأثير مفيد على جوانب الحياة السياسية لبلد مستهدف ذات أهمية، وسياسته الخارجية، وحل المشاكل الدولية، وتضليل الخصم".

من حيث طول العمر، كانت التدابير الفعالة عنصرًا أساسيًا في السياسة الروسية لقرون. وقبل 100 عام من بدء الحرب الباردة، استخدمت الشرطة السرية القيصرية مجموعة واسعة من التدابير الفعالة لقمع جماعات المعارضة الداخلية واختراق منظمات المعارضة المهاجرة في بلدان أخرى.

بعد عقود، اعتمد البلاشفة بشكل كبير على مزيج من الدعاية وأساليب التأثير السياسي للترويج لأجندتهم السياسية. ويذكر الباحثان شولتز وجودسون أن هذا المزيج الفريد من أساليب التأثير السري هو ما أدى إلى "تطور منطقي" لأساليب "التدابير الفعالة" السوفيتية

خلال الحرب الباردة. ومع نظام تلو الآخر، وديكتاتور تلو الآخر، أصبحت ممارسة "التدابير الفعالة" في نهاية المطاف جزءًا لا يتجزأ من ثقافة الاستخبارات الروسية، وأدى تأثيرها الكبير في العلاقات الأمريكية – السوفيتية إلى قيام رونالد ريغان بإنشاء فريق عمل "التدابير الفعالة".

وكانت مهمة المجموعة البحث عن تدابير فعّالة واقتراح طرق يمكن لأمريكا من خلالها مواجهة آثارها السلبية. وفي تقرير صدر عام 1987، حدد باحثون من مجموعة العمل المعنية بالتدابير الفعالة بعضًا من أكثر تقنياتها شيوعًا. وتضمنت قائمتهم استخدام جماعات واجهة، وبثًا سريًا، وتزويرًا، وعملاء نفوذ، وتلاعبًا، وتضليلًا، ودعاية علنية.

وبصرف النظر عن هذه التدابير "الناعمة"، أشارت مجموعة العمل المعنية بمكافحة الإرهاب إلى أن التدابير الفعالة قد تمتد أيضًا إلى أنشطة أكثر عنفًا، وضمنها العمليات السرية الرامية إلى التحريض والاغتيالات المستهدفة والإرهاب. وفي أحد أهم تقاريرها الصادر عام 1987، كتبت مجموعة العمل المعنية بـ "التدابير الفعالة"، أنها "تختلف عن التجسس ومكافحة التجسس، وعن الأنشطة الدبلوماسية والإعلامية التقليدية".

بينما ينطوي التجسس تقليديًا على قيام ضابط مخابرات بجمع معلومات تتعلق بالدول الأجنبية سرًا، فإن

"التدابير الفعالة" تنطوي على قيام ضابط أو عميل بنشر المعلومات (علانية وسرية) بهدف التأثير في الدول الأجنبية والشركات والأفراد.

وفي الحرب الباردة، كانت "التدابير الفعالة" من مسؤولية الخدمة (أ) ضمن المديرية الرئيسة الأولى للجنة الحكومية (كي. جي. بي.)، كما نسقت الخدمة (أ) العمليات مع الإدارة الدولية التابعة للجنة المركزية للحزب الشيوعي السوفيتي.

وفي تقرير صدر عام 1987، قدّر محللو الاستخبارات الأمريكية أن هناك ما يصل إلى 15000 ضابط في (كي. جي. بي.) مخصصون لـ "جهود التضليل والحرب النفسية" (وهما ممارستان تندرجان تحت "التدابير الفعالة". أما فيما يتعلق بالجداول اليومية لموظفي (كي. جي. بي.)، فقد أفاد فاسيلي ميتروخين بأن ضباط العلاقات العامة (ضباط كي. جي. بي. المتمركزين في أماكن إقامة أجنبية) كانوا مطالبين بتخصيص 25% من وقتهم للتدابير النشطة.

وفيما يتعلق بتمويل هذه الأنشطة، قدرت وكالة المخابرات المركزية أن (كي. جي. بي.) أنفق 4 مليارات دولار سنويًا في ثمانينات القرن الماضي على "التدابير الفعالة" (ما يعادل تقريبًا 8.5 مليار دولار بأسعار اليوم).

ومن المهم ملاحظة أنه بينما لا يزال الصحفيون والأكاديميون في العالم الناطق بالإنجليزية يستخدمون مصطلح: "التدابير الفعالة"، تم التخلي عن استخدامه في بلده الأصلي واستُبدل بمصطلح: "تدابير الدعم". وبحسب باحثين من المركز الدولي للدفاع والأمن، فإن الاستخدام العام للمصطلح الأحدث يعود إلى وثيقة قانونية صدرت عام 1992.

ومع ذلك، ورغم تغيير المصطلحات، خلص باحثو المركز الدولي لدراسات الدفاع إلى أن "تدابير الدعم هي الوريث المباشر لـ "التدابير الفعالة"، وهي مجرد مصطلح جديد وصحيح سياسيًا صياغ بعد سقوط الاتحاد السوفيتي".

السمات المميزة لـ "التدابير الفعالة"

رغم أن الولايات المتحدة تنفذ عمليات نفسية، إلا أن هذه العمليات عادة تُدرج ضمن التعريف الأمريكي لـ "التدابير السرية"، ولا يشمل الممارسات الروسية العلنية النموذجية للدعاية ووسائل الإعلام التي ترعاها الدولة.

وبالمثل، تمتلك المديرية العامة الفرنسية للأمن الخارجي قسم العمليات" الذي ينفذ بعض ما يعتبره الأمريكيون "عمليات سرية"، لكنه أقرب إلى العمليات

العسكرية الخاصة لقوات البحرية الأمريكية منه إلى عمليات الاستخبارات.

وبغض النظر عن الاختلافات في المصطلحات، هناك خصائص مختلفة تميز مفهوم "التدابير الفعالة" الروسية عن عقيدة العمل السري لنظيراتها الغربية. ومن السمات المميزة مسألة متى يتم تطبيقها، أو بشكل أكثر تحديدًا، متى ترى كل ثقافة أنه ينبغي تطبيقها.

والتقاليد السوفيتية توفر مبررًا راسخًا لتطبيق "التدابير الفعالة" في أي سياق تقريبًا. كما يوضح ليونارد شابيرو، "إن استخدام وجود عسكري هائل وأقصى قدر من التجسس والتخريب جزء مما يوصف دائمًا في المصطلحات السوفيتية بأنه "صراع أيديولوجي"، وهو ما يُؤكده مرارًا وتكرارًا باعتباره شرطًا ضروريًا لـ"التعايش السلمي".

ورغم أنها محجوبة إلى حد كبير عن أنظار العامة، تخضع العمليات السرية الأمريكية لمتطلبات إبلاغ قانونية صارمة، كما هو منصوص عليه في تعديل هيوز-ريان لعام 1974 وقانون تفويض الاستخبارات لعام 1991. وينص تعديل هيوز-ريان تحديدًا على إلزام وكالة المخابرات المركزية بالإبلاغ عن جميع العمليات السرية إلى ما لا يقل عن 8 لجان في الكونغرس (4 في كل مجلس)، وهو ما يعادل حوالي 60 عضوًا في الكونغرس.

في روسيا الحديثة، أفاد الجاسوس السوفيتي السابق ألكسندر ليتفينينكو أنه عند حل جهاز المخابرات السوفيتية (كي. جي. بي.) لم يعد جهاز المخابرات الروسي خاضعًا لرقابة الحزب الشيوعي، وبدأت مختلف الأجهزة الأمنية "بالعمل في روسيا بشكل مستقل تمامًا ودون أية رقابة".

تقنيات التدابير الفعالة

رغم اتساع نطاق التدابير الروسية الفعالة، إلا أن بعض التقنيات حظيت باهتمام جماهيري أكبر من غيرها، وتتميز 4 تقنيات ليس فقط باستخدامها الواسع لكن أيضًا باستخدامها تحديدًا ضد الانتخابات الرئاسية الأمريكية. وتشمل هذه الأساليب:

- عملاء النفوذ.
- الجماعات الواجهة.
- الابتزاز.
- التزوير.

ولأن هذه المصطلحات من المحتمل أن تكون غير مألوفة لأي شخص خارج مجتمع الاستخبارات، فسوف نفحص كل مصطلح على حدة قبل تحليل تطبيقاته ضمن دراسات حالة محددة.

وكلاء النفوذ

أولًا، عند تعريف عملاء النفوذ، من المهم التمييز بينهم وبين عملاء التجسس التقليديين، تمامًا كما ميّزت مجموعة العمل المعنية بمكافحة التجسس بين "التدابير الفعالة" وأنشطة التجسس "التقليدية". ووفقًا لتقرير صادر عن مجموعة العمل المعنية بمكافحة التجسس عام 1992، فإن "عملاء النفوذ هم أجانب جندتهم المخابرات السوفيتية (كي. جي. بي.) لاستخدامهم في التأثير في آراء الرأي العام والحكومات الأجنبية". وبينما يقتصر دور عملاء التجسس التقليديين على جمع المعلومات المتعلقة بالأحداث الجارية حول العالم، فإن عملاء النفوذ مكلفون بدور أكثر فاعلية في تغيير مجريات الأحداث العالمية. ومع ذلك، في كلتا الحالتين، فإن انتماء العميل إلى وكالة استخبارات أجنبية يبقى سريًا.

خلال الحرب الباردة، كانت عمليات عملاء التأثير من أكثر عمليات "التدابير الفعالة" صعوبة في تحديدها، حيث كان يُنظر إلى العديد من عملائها كوطنيين مخلصين يعبرون عن آراء خاصة بهم تمامًا. وعملاء النفوذ كانوا يُكلَّفون في أحيانٍ كثيرة بالعمل داخل دوائرهم الاجتماعية الخاصة.

جماعات الواجهة

تُستخدم الجماعات الواجهة أو المنظمات الواجهة أيضًا لممارسة النفوذ على دولة أو مجموعة من الأشخاص أو فرد، وغالبًا تكون ذات طبيعة سياسية. مع ذلك، قد تدّعي بعض الجماعات الواجهة أنها منظمات خيرية أو اجتماعية. وبغض النظر عن وظيفتها، فإن هذه الجماعات لا ترتبط علنًا بالحكومة الروسية.

الابتزاز

هناك أسلوب أكثر عدوانية يتمثل في الابتزاز (أو المعلومات المحرجة). وعندما كانت إحدى عمليات الحرب الباردة تتطلب اتخاذ تدابير هجومية أكثر ضد شخص أو مجموعة أشخاص، كان (كي. جي. بي.) يلجأ في كثير من الأحيان إلى جمع المعلومات المحرجة لتوفير الآلية اللازمة لإسقاطه سريعًا أمام الرأي العام. وتضمنت مصادر المعلومات المحرجة التي شُجع عملاء (كي. جي. بي.) على البحث عنها الماضي الخفي، والعادات الخاصة، أو أية سمات شخصية يمكن اعتبارها منحرفة اجتماعيًا.

وعندما يتعذر العثور على أية مواد إحراجية، كان يتم اختلاقها ونشرها عبر أية وسيلة إعلامية تقبلها كحقيقة. والابتزاز كان وما يزال ممارسة راسخة وشائعة في الحرب السياسية الروسية، حتى أن هناك اليوم موقعًا

إلكترونيًا مخصصًا لتوثيق القصص الفاضحة التي يجمعها الخصوم السياسيون.

التزوير

من أجل تقديم معلومات محرجة ملفقة أو أي أكاذيب أخرى من شأنها أن تفيد المصالح الخارجية لروسيا، غالبًا يلجأ جهاز المخابرات الروسي إلى التزوير. ويمكن أن تخدم عمليات التزوير أغراضًا لا حصر لها، لكنها عادة تكون موجهة نحو أحد غرضين:

- تلفيق "أدلة" تشهيرية ضد هدف.
- تزييف وثائق حكومية رسمية تشير إلى ارتكاب مخالفات من جانب دولة.

كان النوع السابق من التزوير يستخدم في أحيانٍ كثيرة لتعزيز المعلومات المشكوك فيها. ووصف لاديسلاف بيتمان النوع الأخير بأنه "نسخ 'محسّنة' قليلًا من وثائق حكومية أصلية تم توزيعها عبر مجهول".

والعديد من المنشقين السوفيت، ومنهم فاسيلي ميتروخين وسيرغي كوندراشيف، وصفوا الولايات المتحدة بأنها: "العدو الرئيس" أو "الهدف الرئيس" لحملات "الإجراءات الفعالة" التي شنّها (كي. جي. بي.)، حتى في ذروة الانفراج الدولي.

وفي مؤتمر لكبار ضباط (كي. جي. بي.) في يناير 1984، نوقشت أهداف "التدابير الفعالة"، وكان يُنظر إلى استغلال الانقسامات الداخلية التي مزقت النسيج الاجتماعي للولايات المتحدة على أنه أحد أكثر الطرق فعالية لإضعاف "العدو الرئيس" من الداخل.

على مدار القرن 20، استخدمت المخابرات (كي. جي. بي.) إجراءات فعالة ضد مجموعة متنوعة من الأهداف، بما في ذلك مارتن لوثر كينغ، وجيه إدغار هوفر، والعديد من المسؤولين السياسيين الأمريكيين الذين دعموا الإجراءات المعادية للسوفيت في أروقة الكونغرس.

"التدابير الفعالة" والانتخابات الرئاسية الأمريكية

إضافةً إلى تقويض السياسة الخارجية الأمريكية والمجتمع الداخلي، اعتبر (كي. جي. بي.) الانتخابات الرئاسية الأمريكية هدفًا مشروعًا في مجال التدخلات العسكرية. ومع ذلك، وبحسب مستوى العداء الأمريكي المُتصوَّر، كان من الممكن أن يكون جهاز المخابرات السوفيتية متحفظًا استراتيجيًا.

وقد كتب السفير السوفيتي أناتولي دوبرينين أنه رغم أن المكتب السياسي الشيوعي كان على دراية تامة

بالانتخابات الرئاسية الأمريكية وتأثيرها في العلاقات الأمريكية السوفيتية، إلا أن المكتب السياسي لم يتدخل قط أو يعرب عن تفضيله علنًا، لأن ذلك قد يكون له تأثير سلبي أكثر من تأثيره الإيجابي. ومن ناحية أخرى، حاولت (كي. جي. بي.) التأثير في الانتخابات الأمريكية من خلال حملات مختلفة للتدابير النشطة، وكان معظمها محددود النجاح.

وفي عام 1960، اتخذ النفوذ السوفيتي على الانتخابات الأمريكية شكل هدايا وكافيار واقتراح لتقديم دعم مالي للمرشح الرئاسي الفاشل مرتين أدلاي ستيفنسون. كان ستيفنسون، المعروف بموقفه الحازم ضد تجارب الأسلحة النووية، يُنظر إليه على أنه شديد التماهي مع المصالح السوفيتية. وعند التواصل مع ستيفنسون في يناير 1960، شكر السفير السوفيتي ميخائيل مينشيكوف على تقدير السوفييت لآرائه، لكنه وصف هذا النهج، أمام دائرته المقربة وفي مذكراته، بأنه "غير لائق للغاية، وغير حكيم، وخطير".

في عام 1968، كُلِّف السفير دوبرينين بمهمة التواصل مع المرشح الديمقراطي هوبرت همفري وعرض عليه دعم حملته الانتخابية بهدف منع نيكسون، المعروف بمواقفه المعادية للسوفيت والشيوعية، من الوصول إلى البيت الأبيض. ورفض همفري، وانتُخب

نيكسون، ما أثار استياء القيادة السوفيتية. لكن سياسة نيكسون أثبتت أنها أفضل بكثير مما توقعه القادة السوفييت. لكن محاولتهم للتهدئة لم تدم طويلًا، عندما تم عزل نيكسون بسبب أفعال اعتبرها دوبرينين "أمرًا طبيعيًا إلى حد ما"، من يهتم إن كان ذلك انتهاكًا للدستور؟

في مذكراته كتب دوبرينين أن سياسيًا أمريكيًا آخر أصبح تحت أنظار المكتب السياسي في 1976. كان لدى الديمقراطي المحافظ هنري ("سكوب") جاكسون سجل سياسي حافل بمعارضة الاتحاد السوفيتي، لا سيما فيما يتعلق بسياساته المتعلقة بهجرة اليهود، وبدا أنه على وشك الحصول على ترشيح الحزب الديمقراطي للرئاسة.

وكتب مارك كرامر من منظمة بونارس أوراسيا أنه بعد فوز جاكسون في الانتخابات التمهيدية في ماساتشوستس ونيويورك، شنّ (كي. جي. بي.) رسميًا حملة إجراءات فعّالة ضده لمنعه من الوصول إلى البيت الأبيض.

تمحورت الحملة بشكل أساسي حول استخدام مواد محرجة ملفقة لتصوير جاكسون على أنه مثلي الجنس يخفي ميوله. ووصل الأمر بعملاء (كي جي بي) إلى حد إرسال رسائل مزورة منسوبة إلى مكتب التحقيقات الفيدرالي إلى العديد من الصحف والصحفيين الأمريكيين، تتضمن "أدلة" ذات صلة بميوله الجنسية. وكان (كي جي بي) مصممًا على منع جاكسون من دخول البيت الأبيض،

حتى أنه بعد انسحابه من السباق الرئاسي، استمر في حملة التضليل الإعلامي ضده.

وحتى ترشحه لإعادة انتخابه رئاسيًا في عام 1984، تمكن رونالد ريغان من تجنب أكثر التكتيكات عدوانية على طيف "التدابير الفعالة" لـ (كي. جي. بي.). لكن عندما اقترب بشكل خطير من الحصول على ترشيح الحزب الجمهوري في عام 1976، كتب ميتروخين أن جهاز المخابرات السوفيتية (كي. جي. بي.) بدأ البحث عن معلومات محرجة ضد حاكم كاليفورنيا، الذي لم يروج قط لأي شيء قريب من الانفراج الدولي في أي من خطاباته السياسية.

فشل ريغان في الفوز بترشيح الحزب الجمهوري عام 1976، وبدلًا من ذلك، أدى جيمي كارتر، الذي بدا مسالمًا، اليمين الدستورية كرئيس للولايات المتحدة الأمريكية، لكنه كان برفقة مستشار الأمن القومي المتشدد، زبيغنيو بريجنسكي، الذي كان يوجهه ويرشده.

في عام 1980، كان (كي. جي. بي.) "أقل انخراطًا" في محاولة التأثير في الانتخابات الرئاسية مقارنةً بما كان عليه قبل 4 سنوات، وذلك لأنهم (على حد تعبير السفير دوبرينين) "سئموا من كارتر وشعروا بالقلق إزاء ريغان".

بدون دعم كبير من الناخبين وبدون حملات تشويه سوفيتية، تمكن ريغان من الفوز بترشيح الحزب الجمهوري والرئاسة. ومع ذلك، خلال فترة ولاية ريغان

الأولى عندما أتبع خطابه المعادي للسوفيت في حملته الانتخابية بإجراءات تنفيذية قوية، وجد نفسه مرة أخرى في مرمى نيران (كي. جي. بي.).

وفي 25 فبراير 1983، أعلن المركز (مقر المخابرات السوفيتية) أنه سيطلق حملة استخباراتية مكثفة ومتعددة القنوات لمنع إعادة انتخاب ريغان، وأمها ستتألف في معظمها من البحث عن مصادر معلومات محرجة وإيجاد جميع الوسائل الممكنة لنشرها. وفي النهاية، فاز فوزًا ساحقًا في انتخابات عام 1984 وأظهر المدى المحدود لآلية نفوذ (كي. جي. بي.). وفيما يتعلق بحملات التدابير النشطة، ستكون هذه آخر محاولة للتأثير على الانتخابات الأمريكية لسنوات.

التدابير النشطة الحديثة

في تسعينات القرن الماضي، في عهد الرئيس يلتسين، تم تفكيك (كي. جي. بي.) كما لو كان بيتًا من ورق، وأعيد توزيع كوادره على أجهزة متفرقة. ولسنوات بعد انتهاء الحرب الباردة، اتخذت حكومة يلتسين قرارًا استراتيجيًا باستغلال الصراع الإقليمي من أجل فرض النفوذ، بدلًا من تخصيص أموال الحكومة الروسية الهشة لحملات دعائية خارجية ضخمة.

في ظل حالة من التخبط والغموض التي تعصف بأجهزة المخابرات الروسية، استقال يلتسين في 31 ديسمبر 1999. وبعد فترة وجيزة من استقالته، أُعيدت "التدابير الفعالة" إلى الحياة على الفور تقريبًا بفضل أحد قدامى المحاربين في (كي. جي. بي.) الذي خدم 16 عامًا، ووجد نفسه في البداية رئيسًا للوزراء بالوكالة، ثم رئيسًا منتخبًا لروسيا. لا يمكن مناقشة عودة الإجراءات الروسية النشطة دون التطرق إلى الرئيس فلاديمير بوتين.

منذ فوزه في انتخابات عام 2000، أنشأ بوتين ما وصفته أولغا كريشتانوفسكايا وستيفن وايت بـ: "العسكرية" من خلال حشد الحكومة الروسية بموظفين سابقين في أجهزة أمن الدولة. وعكست عملية إعادة تنظيم السلطة المعقدة التي قام بها بوتين ثقافة الحرب الباردة التي سادت بين أسلافه إلى درجة أن البعض وصف نظامه بأنه دولة (كي. جي. بي.). وسواء أكان يستخدم إجراءات فعّالة لمهاجمة الأنظمة الديمقراطية، أو إضعاف التحالفات السلمية عبر الأطلسي، أو استغلال الصراعات الداخلية في الدول الأخرى لتزويد روسيا بمزيد من القوة والمزايا السياسية على الساحة الدولية، يبدو أن بوتين قد دمج عقيدة (كي. جي. بي.) في ممارسات الاستخبارات الروسية الحديثة.

إحدى أكثر الطرق فعالية التي استخدمتها أجهزة الاستخبارات الروسية الحديثة لتحقيق ذلك، الاستفادة من أدوات الإنترنت الجديدة لمهاجمة الدول المعادية خلال مواسم الانتخابات. وأظهرت العديد من الديمقراطيات أعراضًا لما تعتقد أنه ناتج عن التدخل الروسي في عملياتها الانتخابية.

لأغراض دراستنا، فإن أهم حالة للتدخل الروسي في الانتخابات بعد الحرب الباردة حدثت في عام 2016 خلال الانتخابات الرئاسية الأمريكية. ورغم أن المحاولات السابقة للتأثير في انتخابات ما بعد الحرب الباردة كانت عمليات هادئة لحملات دعائية صغيرة النطاق، إلا أن الانتخابات الرئاسية الأمريكية لعام 2016 أظهرت استعراضًا غير مسبوق للقوة، الأمر الذي صدم العديد من الدول الأخرى ودفعها إلى تعزيز أمن عملياتها الانتخابية.

لطالما صعّبت الطبيعة السرية المتأصلة في "التدابير الفعالة" على الباحثين (وبخاصة من هم خارج مجتمع الاستخبارات) التحقق من تأثيرها في الأحداث الجارية وإصدار أحكام قاطعة بشأنه. إضافةً إلى ذلك، فإنّ نقص روايات المنشقين بعد الحرب الباردة وكتيبات أجهزة الاستخبارات الروسية يحدّ من عدد المصادر الأولية المستخدمة للتحقق.

ورغم هذه القيود، أكدت تقييمات استخباراتية مختلفة وتقارير الأمن السيبراني وشهادات الكونغرس جميعها التقييم القائل بأن الانتخابات الرئاسية الأمريكية لعام 2016 كانت أحدث وأكثر مظاهر الإجراءات الروسية النشطة الموجهة ضد الولايات المتحدة تدميرًا. ولا شك أيضًا في أنه مع ظهور الأدوات السيبرانية، اتسع نطاق تكتيكات التدابير النشطة أكثر مما كان عليه خلال الحرب الباردة.

مع قيام الحكومات بالتحقيق في حالات النفوذ الاستخباراتي الروسي الحديثة، أصبح المزيد من المعلومات متاحًا الآن لإجراء البحوث المقارنة. كما جهات عديدة: مراكز فكر ومنظمات غير حكومية ومنظمات دولية بتخصيص رأس المال مادي وبشري لتحديد تكتيكات "التدابير الفعالة" في القرن 21.

دراسة حالة رقم 1: الانتخابات الرئاسية الأمريكية لعام 1984

خلفية

تتعلق دراسة الحالة الأولى لدينا بسباق رونالد ريغان الرئاسي الأمريكي عام 1984 و"الإجراءات الفعالة" التي اتخذها (كي. جي. بي.) في محاولة لمنع إعادة انتخابه. رغم تصعيد الإجراءات السوفيتية واستهدافها بشكل خاص ضد ريغان في عام 1984، إلا أن (كي. جي. بي.) كان يراقب مسيرة السياسي الكاليفورني لسنوات قبل إعادة انتخابه.

كان خطاب ريغان العلني معاديًا للسوفيت بشكلٍ سافرٍ لدرجة أن المركز اعتقد أنه انتخابه قد يعني ضربةً نوويةً أمريكية. واستعدادًا لمثل هذا الوضع، شرع (كي. جي. بي.) في سلسلة إجراءات غير مباشرة، تضمنت في معظمها جمع معلومات محرجة. وتوقفت هذه الجهود عندما خسر ريغان ترشيح الحزب الجمهوري.

بعد سنوات، عندما عُرض (كي. جي. بي.) خياران: إما الرئيس ريغان المناهض للشيوعية، أو مستشار الأمن القومي زبيغنيو بريجنسكي، الذي كان مناهضًا بشدة للسوفيت في عهد جيمي كارتر، وجد الجهاز نفسه في مأزق. في نوبة غير معهودة من التحفظ، انتظرت القيادة السوفيتية على الهامش لمعرفة من سيفوز في الانتخابات، وندم (كي. جي. بي.) لاحقًا على هذا القرار، إذ اتخذ رونالد ريغان موقفًا أكثر عدائية تجاه الاتحاد السوفيتي من سلفه الديمقراطي.

بعد ضبط النفس الاستراتيجي الذي أبدته المنظمة وامتناعها عن استخدام "تدابير فعّالة" خلال الانتخابات الرئاسية لعام 1980، كان الهدف الأول للمركز في انتخابات عام 1984 واضحًا: منع رونالد ريغان من الفوز بولاية ثانية. وخلص فاسيلي ميتروخين إلى أن الرغبة الشديدة في تشويه سمعة إدارة ريغان هي التي دفعت رئيس (كي. جي. بي.) إلى الإعلان في 12 أبريل 1982 أنه يتعين على جميع ضباط المخابرات الأجنبية الآن المشاركة في "التدابير الفعالة".

بعد مرور عام تقريبًا، وتحديدًا في 25 فبراير 1983، أعلن المركز أنه سيطلق حملة فعّالة متعددة القنوات تستهدف رونالد ريغان تحديدًا. تمت الموافقة على نشر معلومات محرجة جُمِعَت مسبقًا عن ريغان وظلت غير مستخدمة لسنوات عبر قنوات الإعلام الجماهيري. كما خلص المركز إلى أن ريغان كان يمتلك "قدرات فكرية ضعيفة"، لكن هذا لم يكن مبدًا أساسيًا في معظم موادهم المناهضة لريغان. ولاقت بعض التقارير الإعلامية السلبية في الخارج، لكنها في نهاية المطاف فشلت في ترسيخ وجودها في الولايات المتحدة.

وكلاء النفوذ

لتعزيز ما تبقى من معلومات محرجة كانت بحوزة (كي. جي. بي.) عن ريغان، استعان المركز بمكاتبه الأمريكية الثلاثة في: واشنطن ونيويورك وسان فرانسيسكو. وكان هناك رغبة قوية في العثور على أي معلومات ذات صلة بريغان وتوفير قنوات شخصية لنشرها.

لسوء الحظ، تفتقر المصادر الأولية إلى معلومات كافية فيما يتعلق بفعالية أي من عمليات التأثير في عام 1980. ومع ذلك، فإن عدم الإبلاغ يشير إلى أن هذا الشرط إما لم يتم الوفاء به أو لم يؤتِ ثمارًا تذكر، حيث لم يتقدم أي من عملاء النفوذ ولم تنشر أي من الحملتين أي تقارير بشأن العملاء السوفيت المشتبه بهم بعد الانتخابات.

جماعات الواجهة

بالإضافة إلى المعلومات المحرجة وعملاء النفوذ، استخدم (كي. جي. بي.) أيضًا جماعات واجهة لعرقلة فرص ريغان في إعادة انتخابه. كانت فائدة استخدام الجماعات الواجهة تكمن في أنه على غرار عملاء النفوذ السوفييت، ظلت صلاتهم بالمركز غامضة، لكن تغطيتهم الجغرافية ونفوذهم السياسي يمكن أن يوفرا مزايا واضحة لأية حملة تشويه سوفيتية. وأمر (كي. جي. بي.) جماعاته الواجهة بنشر الشعار السياسي: "ريغان يعني الحرب!"

والجهود السوفيتية في هذه الحملة فشلت في التأثير على الفئة الديموغرافية الرئيسة للناخبين الأمريكيين.

بحسب إدموند موريس، كاتب سيرة ريغان، فقد نجح ريغان في التأثير في الشعب السوفيتي عندما وصف الاتحاد السوفيتي صراحةً بأنه: "إمبراطورية شريرة" في خطاب ألقاه في 9 مارس 1983. وخلال ساعات، أفاد غربيون في موسكو بأن ردة فعل من "الاشمئزاز الذاتي والاعتراف بالحقيقة" انتشرت في جميع أنحاء المجتمع الروسي ضد حكومتهم.

التزوير

كان نشر المعلومات المزورة تكتيكًا شائعًا لـ "التدابير الفعالة". وفي كتاب "تعليمات من المركز"، يشير كريستوفر أندرو وأوليغ غوردييفسكي إلى أن تزويرات الجهاز "أ" ضد إدارة ريغان كانت بشكل عام من نوعين:

- "تزويرات صامتة " تُعرض بسرية على قادة العالم الثالث.
- تزويرات علنية في حملات إعلامية.

خلال ولايته الأولى، كان ريغان هدفًا لعمليات تزوير متكررة، ولعلّ أشهرها رسالة ملفقة إلى ملك إسبانيا، تحثّ الزعيم الأوروبي على الإسراع في: "إزالة القوى التي تعرقل انضمام إسبانيا إلى حلف شمال الأطلسي". أُرسلت

نسخ من هذه الرسالة بالبريد إلى الصحفيين الإسبان، وكذلك إلى جميع المندوبين (باستثناء الأمريكيين) الذين حضروا مؤتمر مدريد للأمن والتعاون في أوروبا. وأشارت الرسالة إلى مذكرة "سرية للغاية" لفقها (كي. جي. بي.) أيضًا، وجرى تداولها مع الرسالة. وبسبب أسلوبها الركيك، لم يكن للرسالة تأثير يُذكر، بل اتهمها العديد من الصحفيين الإسبان علنًا بأنها سوفيتية المصدر.

ملخص

فشلت حملة التدابير النشطة في انتخابات عام 1984 في التأثير على شعبية ريغان لدى الناخبين الأمريكيين. ومثل العديد من حملات "التدابير الفعالة" الأخرى خلال الحرب الباردة، بالغ (كي. جي. بي.) في تقدير فعاليتها. ويشير كريستوفر أندرو كذلك إلى أن "محدودية هذه التدابير تجلت في الفشل في نشر الشعار الرئيس: "ريغان يعني الحرب!" أية دولة من دول الناتو.

فاز ريغان في 49 ولاية من أصل 50 في المجمع الانتخابي، ما ضمن له ولاية ثانية وموارد إضافية لدعم سياساته المناهضة للسوفيت.

دراسة حالة رقم 2: الانتخابات الرئاسية الأمريكية لعام 2016

خلفية

في عام 2016، وبعد أكثر من 30 عامًا على الانتخابات الرئاسية الأمريكية لعام 1984، توجهت أمريكا إلى صناديق الاقتراع لانتخاب رئيس جديد. وخلال هذه الدورة الانتخابية، كان هناك 3 مرشحين أساسيين: الجمهوري دونالد ترامب، والديمقراطية هيلاري كلينتون، وبيرني ساندرز.

وكما هو الحال مع حملة التدابير النشطة خلال انتخابات عام 1984، فقد تم التخطيط لـ "التدابير الفعالة" الموجهة نحو انتخابات عام 2016 قبل يوم الانتخابات بوقت طويل. وكما حدث في عام 1984، بدأت هذه التدابير الناعمة في شكل جمع المعلومات السرية.

في سبتمبر 2015، اتصل مكتب التحقيقات الفيدرالي باللجنة الوطنية الديمقراطية لإبلاغها بأن أحد أجهزة الكمبيوتر التابعة لها اخترقته جهة روسية متخصصة في الهجمات الإلكترونية. وفي نوفمبر 2015، تواصل مكتب التحقيقات الفيدرالي (FBI) مجددًا مع اللجنة الوطنية الديمقراطية (DNC) للإبلاغ عن أن أحد

أجهزة الكمبيوتر التابعة لها كان يرسل معلومات بنشاط إلى روسيا. وفي 14 يونيو 2016، ذكرت صحيفة واشنطن بوست أن قراصنة روس تمكنوا من الوصول إلى خوادم اللجنة الوطنية الديمقراطية، والتي تضمنت وثائق تتعلق بأبحاث المعارضة حول دونالد ترامب. وبعد يوم، أعلن مدوّن مجهول يُدعى غوتشيفر مسؤوليته عن الاختراق، زاعمًا أنه ناشط إلكتروني روماني لا ينتمي إلى المخابرات الروسية.

بعد أسبوع، نشر موقع ويكيليكس ما يقرب من 20 ألف رسالة بريد إلكتروني على الإنترنت تم تسريبها من خادم اللجنة الوطنية الديمقراطية. رغم إمكانية استخدام القرصنة الإلكترونية لأغراض إجرامية واستخباراتية متنوعة، إلا أن الاستهداف المتعمد للرسائل الإلكترونية والوثائق الشخصية من خادم اللجنة الوطنية الديمقراطية ونشرها لاحقًا، وصفه الكثيرون بأنه مثال واضح على الابتزاز الإلكتروني.

في ديسمبر 2016، اكتُشِف أن العديد من خوادم الحزب الجمهوري اختُرِقَت وجرى استخراج البيانات منها. إلا أن هذه الوثائق لم تُنشر قط؛ وهو ما دعم تقييمًا لاحقًا لمجتمع الاستخبارات الأمريكية مفاده أن حملة النفوذ الروسي سعت إلى تشويه سمعة هيلاري كلينتون بدلًا من دونالد ترامب.

وكلاء النفوذ

كوسيلة لنشر المعلومات المُحرجة التي جمعتها، استخدمت روسيا نسخًا رقمية متعددة من عملاء التأثير التقليديين. ووفقًا لتقرير مجتمع الاستخبارات الأمريكي بعنوان: "التدخل الروسي في انتخابات 2016"، فقد دمجت روسيا هذه التقنية في استراتيجية تواصل طويلة الأمد تضمنت تاريخيًا مزيجًا من عملاء التأثير والواجهات والمنظمات الصورية.

في عام 2016، تضمن ذلك على وجه التحديد استخدام "وسطاء من أطراف ثالثة ومستخدمي وسائل التواصل الاجتماعي المدفوع لهم أو "المتصيدين". كانت أغلبية هذه الحسابات شخصيات وهمية على الإنترنت أنشأتها وكالة أبحاث الإنترنت، وهي شركة يملكها يفغيني بريغوجين، أحد أصدقاء فلاديمير بوتين المقربين. وأجرت عدة وسائل إعلام مقابلات مع موظفين سابقين في وكالة أبحاث الإنترنت، ممن عملوا في "مصانع التضليل" الروسية سيئة السمعة، حيث كان الموظفون يتلقون تعليمات حول كيفية انتحال شخصية أمريكيين حقيقيين، ثم نشر محتوى على وسائل التواصل الاجتماعي يخدم أجندة روسيا الخارجية والداخلية.

بينما ادّعت شخصيات أنها أمريكية، مثل جينا أبرامز، الشخصية الجنوبية اليمينية على تويتر، ادّعى آخرون أنهم أجانب يسعون إلى الحقيقة وسط الانتخابات الأمريكية، مثل غوتشيفر 2.0. بالإضافة إلى الشخصيات المزيفة البارزة، كان هناك الآلاف من وكلاء التأثير الآليين، والمعروفين أيضًا باسم "الروبوتات"، الذين أنشأتهم وكالة أبحاث الإنترنت، والذين تم نشرهم في الغالب للتغريد وإعادة التغريد على منصة التواصل الاجتماعي تويتر.

أظهرت دراسة أجرتها شركة الأمن السيبراني "فاير آي" أن برامج الروبوت الروسية نجحت في جعل أحد الوسوم الروسية المزيفة #HillaryDown مدرجًا ضمن الوسوم الرائجة على تويتر، ما يعني أنه حظي باهتمام جماهيري كافٍ ليظهر على الصفحة الرئيسة لتويتر.

جماعات الواجهة

بالإضافة إلى إنشاء شخصيات وهمية، استخدمت روسيا أيضًا مجموعات واجهة رقمية. أُنشئت معظم المجموعات الوهمية على منصة التواصل الاجتماعي الشهيرة فيسبوك، حيث حصدت عشرات الآلاف من الإعجابات إلى أن قام مشرفو فيسبوك بإزالة صفحات المجموعات. فيما يتعلق بفعاليتهما في التأثير في الناخبين الأمريكيين، تمكنت جماعتان متقابلتان على طرفي نقيض

في قضية الحقوق المدنية من حشد أتباعهما فعليًا للاحتجاج ضد بعضهما البعض خارج مركز إسلامي في هيوستن، تكساس.

إحدى الجماعات الواجهة التي تُدعى "قلب تكساس" كان لديها 250 ألف متابع. أما المجموعة الأخرى التي تمكنت روسيا من حشدها فكانت تُسمى: "مسلمو أمريكا المتحدون"، وكان لديها 328 ألف متابع.

التزوير:

كان الجمع بين كل هذه الأساليب بمنزلة معالجة مبتكرة لأسلوب التزوير. من بين أسلوبي التزوير اللذين استخدما ضد إدارة ريغان، واللذين تضمنا تزويرًا صامتًا تم إرساله إلى قادة العالم وتزويرًا موجهًا لوسائل الإعلام الجماهيرية، فإن تزوير عام 2016 يشبه إلى حد كبير الأسلوب الأخير.

وفي لائحة اتهام رُفعت في 16 فبراير 2018، ذكر المحقق الخاص روبرت مولر وفريقه أن ممثلين روس اشتروا، على الأقل، من أبريل 2016 وحتى نوفمبر 2016 إعلانات على فيسبوك باستخدام شخصيات مزيفة. ثم شرعوا في إنتاج وشراء ونشر هذه الإعلانات المزيفة على مواقع التواصل الاجتماعي الأخرى التي تدعو صراحةً إلى ترامب أو تعارض صراحةً كلينتون.

بدلًا من شعار: "ريغان يعني الحرب!"، كان هناك سيل متواصل من الوسوم (الهاشتاغات) التي أُرفقت بمنشورات مختلفة على وسائل التواصل الاجتماعي. من بين هذه الوسوم:

"#هيلاري_للسجن"

"#لن_أصوت_لهيلاري ".

خلال المراجعة التي فرضها الكونغرس على الحسابات الروسية المزيفة بعد الانتخابات، وجد محللو فيسبوك "ما يقرب من 100 ألف دولار من الإنفاق الإعلاني من يونيو 2015 إلى مايو 2017 - المرتبطة بحوالي 3000 إعلان - والتي كانت متصلة بحوالي 470 حسابًا غير موثوق به.

كما أفادوا بأن الحسابات المزيفة "بدت وكأنها تركز على تضخيم الرسائل الاجتماعية والسياسية المثيرة للانقسام عبر الطيف الأيديولوجي – متناولة مواضيع تتراوح من قضايا المثليين والمتحولين جنسيًا إلى قضايا العرق والهجرة وحقوق حمل السلاح".

ملخص

مع استمرار تداول أنباء التدخل الروسي المزعوم، وجّه الرئيس المنتهية ولايته باراك أوباما أجهزة الاستخبارات لإجراء مراجعة شاملة لما حدث خلال

العملية الانتخابية لعام 2016. بالنسبة لعامة الناس، ربما بدا في البداية أن روسيا لم تستخدم سوى نفوذ سري ضد الانتخابات الرئاسية لعام 2016.

تحليل دراسة الحالة

من خلال دراستي الحالة المذكورتين أعلاه، تظهر العديد من التقنيات الكلاسيكية المشتركة. يُعدّ "الابتزاز" أحد الأساليب التي استخدمتها روسيا لتشويه سمعة المرشحين الرئاسيين الأمريكيين. كما يتضح من دراسات الحالة، فإن استخدام المعلومات المبتزة متشابه في كلتا الحالتين، لكن القدرة على الحصول على هذه المعلومات والقدرة على إنكار المسؤولية قد تعززت بشكل كبير بفضل أدوات القرصنة الإلكترونية.

رغم أن جهاز المخابرات السوفيتية (كي. جي. بي.) كان معروفًا بوجود مجموعات واجهة له في جميع أنحاء أمريكا، وبالتأكيد في واشنطن طوال فترة الحرب الباردة، إلا أنه لم يكن قادرًا دائمًا على تسليم المواد المحرجة التي تطلبها موسكو. كانت هذه الجماعات في حقبة الحرب الباردة تقتصر عادةً على مجموعات من الناس، ما تطلّب وجودًا ماديًا ووجودًا ورقيًا لا مفر منه. أما مجموعات فيسبوك المزيفة العديدة التي أُنشِئت في عام 2016،

فظهرت واختفت، ودون وجود أية وثيقة متاحة للجمهور للتحقق من أصولها.

لكن في عام 2016، عندما بدأت فتاة أمريكية شابة تدعى جينا أبرامز بنشر تغريدات ذات طابع سياسي على تويتر قبيل الانتخابات بفترة وجيزة، حظيت باهتمام كبير من السياسيين والصحفيين والجمهور الأمريكي. دخلت أبرامز في جدالات على تويتر مع السفير الأمريكي السابق لدى روسيا وخبير الدعاية الروسية مايكل مكفول، وأعاد مايك فلين جونيور نشر تغريدتها، كما ذُكرت في تقارير نشرتها صحيفتا واشنطن بوست ونيويورك تايمز.

خاتمة

الانتخابات الرئاسية لعام 2016 ذكّرت مجتمع الاستخبارات الأمريكي والكونغرس بحقيقة التدخل الأجنبي في العمليات الانتخابية الأمريكية، وأطلقت سلسلة من الاستفسارات والتحقيقات والنقاش العام.

مع ذلك، ورغم كل المعلومات الجديدة التي ظهرت، فقد وجدت لجنة مجلس الشيوخ المختارة لشؤون الاستخبارات في يوليو 2018 أن تغطية التقييم الاستخباراتي المشترك الأمريكي لعام 2017 لـ "السياق التاريخي للتدخل الروسي في السياسة الداخلية الأمريكية سطحية".

رغم وجود العديد من الأفكار التي يستطيع المواطنون الأمريكيون وصناع السياسات استخلاصها من أحداث عام 2016 والبحوث التي أجراها الكونغرس لاحقًا، إلا أن هناك جانبًا واحدًا يبرز بشكل خاص. هذا الجانب هو ما أطلق عليه مدير وكالة المخابرات المركزية السابق مايك بومبيو اسم: "الفهم الاستراتيجي" لأساليب "التدابير الفعالة".

خلال الحرب الباردة، أشار العديد من المنشقين السوفيت إلى ضرورة قيام أجهزة الاستخبارات الغربية بإعادة النظر في أساليب الاستخبارات الروسية وتقييمها، وموازنة ذلك مع احتمالية قيام روسيا بأعمال تخريب سياسي. كما يتضح من نتائج مجلس الشيوخ، هناك حاجة عامة للتوعية العامة بتاريخ هذه التدابير على نحو يربط هذا التاريخ بالمستقبل، لا سيما فيما يتعلق بالفضاء الإلكتروني.

قبل أكثر من 30 عامًا من الانتخابات الرئاسية الأمريكية لعام 2016، شارك المنشق السوفيتي لاديسلاف بيتمان بعض التوقعات الثاقبة في كتابه: "كي. جي. بي. والتضليل السوفيتي: نظرة من الداخل"، حيث قال إن أجهزة الكمبيوتر تُعد مصدرًا آخر للبيانات القيّمة لـ (كي. جي. بي.).

إن استخدامها لتخزين ومعالجة ونقل البيانات الحساسة المتعلقة بالأفراد في القطاعات الخاصة، مثل القطاع المصرفي والطبي وقطاعات الإيرادات الحكومية أو الفيدرالية، يفتح آفاقًا جديدة لأجهزة الاستخبارات الشيوعية.

وعملاء (كي. جي. بي.) في الولايات المتحدة مهتمون جدًا بأبحاث التشفير الحاسوبي، سواء العسكرية أو المدنية. والوصول إلى هذا المفتاح السحري سيمكن (كي. جي. بي.) من اختراق خصوصية كل أمريكي تقريبًا دون الانخراط في عمليات محفوفة بالمخاطر وتستغرق وقتًا طويلًا، والأهم من ذلك، أنه سيكون قادرًا على تلويث نظام الحاسوب بمعلومات مضللة عن الأفراد أو الشركات، مما يُلحق ضررًا بالغًا بحياتهم ويُشلّ عملياتهم.

إن انفتاح الإنترنت يفيد الأمريكيين بقدر ما يفيد أعداء أمريكا. وبينما يشارك المتسللون والإرهابيون والجواسيس في كتابة الفصل الحالي من التاريخ المتعلق بالعمليات السرية الرقمية، فمن الضروري أن يكون مواطنو العالم على دراية بمحاولات روسيا التاريخية لتقويض المؤسسات الأمريكية حتى لا تتكرر أخطاء الماضي.

الفصل الثاني
الاستخبارات الإيرانية على وسائل التواصل الاجتماعي

مع تخصيص الكثير من التغطية الإعلامية لروسيا، يجهل العديد من الأمريكيين النطاق الواسع للعمليات التي يقوم بها أحد أكثر خصوم أمريكا إصرارًا في المجال الرقمي: دولة إيران. وعلى مدى العقدين الماضيين، ومن خلال العمل تحت غطاء الجهات الفاعلة بالوكالة والشبكات الخاصة الافتراضية، بنت إيران سمعة كقوة سيبرانية هائلة.

تشتهر إيران في أوساط مجتمع الاستخبارات الأمريكي بشن هجمات إلكترونية وحشية ضد الكيانات الحكومية الأمريكية والشركات والأفراد. وفي السنوات الأخيرة، بدأت إيران تفضل استخدام أسلوب تجسس كلاسيكي محدد في عملياتها الإلكترونية. لقد سمح الإحياء

الرقمي لهذه التقنية للجهات الفاعلة الإلكترونية الخبيثة في إيران ليس فقط باستهداف أنظمة الكمبيوتر والبنية التحتية الحيوية، بل أيضًا البشر.

التقنية التي تدمجها إيران في ترسانتها السيبرانية هي فخ العسل. تتضمن فخاخ العسل عادةً استخدام ضابط مخابرات جذاب معتاد على إغراء الخصوم غير المدركين لمشاركة المعلومات السرية من خلال استغلال علاقة شخصية (وأحيانًا رومانسية). وأصبحت تقنية جمع المعلومات التقليدية المعروفة باسم: "فخ العسل" رقمية، وسرعان ما أصبحت سمة مميزة لاستراتيجية جمع المعلومات الاستخباراتية الإيرانية.

لقد أثر الإنترنت ووسائل التواصل الاجتماعي على الحكومات في جميع أنحاء العالم بطرق مختلفة. وإحدى الطرق التي أثرت بها هذه التقنيات الجديدة على الحكومات هي القدرة على رقمنة المعلومات. وأصبحت الآن الأشكال المادية السابقة للوثائق السرية تُنشأ وتُحرر وتُنشر ضمن بيئات رقمية متصلة بالشبكة، وتتسرب أحيانًا إلى قطاعات مختلفة من المجتمع.

وبصرف النظر عن رقمنة الوثائق السرية، أصبح من الواضح أيضًا أن المظاهر المادية السابقة لهوية ضابط

المخابرات تتجلى الآن في شكل بتات وبايتات، متناثرة عبر الفضاء الرقمي، وفي انتظار أن يكتشفها الخصوم الماهرون في مجال الأمن السيبراني.

لا يوجد مكان يتجلى فيه هذا الأمر أكثر من فضاءات الإنترنت لمواقع التواصل الاجتماعي. ورغم أن العديد من مواقع التواصل الاجتماعي فضحت روسيا بسبب نشاطها الخبيث على الإنترنت، إلا أن إيران تثبت أنها لا تقل خطورة في وسائل التواصل الاجتماعي.

والجهات الفاعلة الإلكترونية الإيرانية تتمتع بالقدر نفسه من المهارة في إقناع مستخدمي وسائل التواصل الاجتماعي بتصديق المعلومات الكاذبة، واختراق أنظمة الكمبيوتر الآمنة، والتسبب في أضرار تتراوح من أضرار طفيفة إلى أضرار جسيمة للأمن القومي الأمريكي.

نظرًا لتزايد استخدام إيران الخبيث لوسائل التواصل الاجتماعي وإثباته أنه يضر بالأفراد والشركات والحكومات، فإنه موضوع جدير بالدراسة بالنسبة لباحثي الاستخبارات المعاصرين.

ويتضمن هذا الفصل دراستي حالة نجح فيهما فاعلون إيرانيون في إشراك مستخدمي وسائل التواصل

الاجتماعي غير المدركين واستخدموا فخاخ العسل الرقمية للوصول إلى معلومات حساسة.

مراجعة الأدب

فيما يتعلق بالبحث حول أساليب الاستخبارات التقليدية وفخاخ الاحتيال الرقمي في وسائل التواصل الاجتماعي، هناك القليل جدًا من الأدبيات مفتوحة المصدر التي تتناول هذين الموضوعين معًا. ومع ذلك، فقد تم تخصيص قدر كبير من الأبحاث لتحليل مواضيع فخاخ العسل التقليدية، وخداع الهوية الرقمية، واستهداف الأفراد عبر الإنترنت (المعروف أيضًا في لغة الإنترنت باسم: "التصيد الاحتيالي الموجه").

مصائد العسل التقليدية

يُعرّف قاموس أكسفورد "فخ العسل" بأنه: "حيلة يقوم فيها شخص جذاب بإغراء شخص آخر للكشف عن معلومات أو القيام بشيء غير حكيم". وضمن هذا التعريف الأوسع، توجد مناهج وأساليب متنوعة استخدمتها وكالات الاستخبارات الأجنبية وحركات المقاومة عبر التاريخ. ورغم أن غالبية المعلومات

الاستخباراتية البشرية يتم جمعها من خلال العلاقات الواقعية القائمة على الألفة، إلا أن فخ العسل يضيف طبقة محددة من الإغراء مصممة خصيصًا للهدف.

من شهرة وإعدام المغرية ماتا هاري في نهاية المطاف، إلى الكادر الأقل شهرة من المغرين الذكور في ألمانيا الشرقية المعروفين باسم: "جواسيس روميو"، تم طبقت دول مختلفة "فخ العسل" بدرجات متفاوتة من النجاح.

وتناول العديد من المؤلفين موضوع فخاخ العسل بشكل غير مباشر كجزء من دراسة تاريخية للنساء في مجال الاستخبارات. ويرجع ذلك على الأرجح إلى الارتباط الثقافي المتأصل بين الإناث وتقنية فخ العسل.

قبل الحرب الباردة بزمن طويل، وبالعودة إلى العصور القديمة، غالبًا ما تم تصوير النساء على أنهن المغويات في عمليات الإيقاع بالنساء. وتُقدّم قصة شمشون ودليلة في الكتاب المقدس سيناريو نموذجيًا لفخ العسل، حيث يقع رجل غير واعٍ في غرام امرأة مكلفة بالحصول على معلومات سرية.

استخدم هذا النموذج الكلاسيكي للمرأة التي تقوم بنصب "فخ العسل" على مدى قرون عديدة وفي ثقافات

مختلفة. وعمليات الإيقاع بالنساء المنظمة التي يعرفها العالم اليوم لم تتطور إلا بعد توظيف ضابطات المخابرات. وقد جادل مؤرخون بأن هذه التقنية الرسمية لجمع المعلومات الاستخباراتية لم تترسخ إلا في الحرب العالمية الأولى، عندما كانت البيروقراطيات الاستخباراتية الحديثة في مهدها. وفي الحربين العالميتين، وُظِّفَت النساء للعب دور حاسم في جمع المعلومات الاستخباراتية. ويعود نجاحهم إلى حد كبير إلى سلوكهم غير المثير للريبة وفهمهم السريع لأساليب التجسس.

بعد أن أفسحت الحربان العالميتان المجال للحرب الباردة، وُجِّهَت عمليات استدراج أكثر تعقيدًا وطويلة الأمد ضد أهداف من الذكور والإناث والمغايرين جنسيًا والمثليين. كانت (كي. جي. بي.) واحدة من أكثر الوكالات شهرة في استخدام أساليب الإغراء الجنسي، حيث استخدمت عملاء ذكور (يطلق عليهم اسم: "الأعمام") لإدارة إما بائعات الهوى أو موظفات المخابرات السوفيتية (يشار إلى كليهما باسم "السنونو").

كُلِّف "الأعمام" بتدريب "السنونو" على أفضل الطرق لإغواء الأهداف الذكورية والحصول على معلومات استخباراتية أجنبية عالية الجودة. وقد تتراوح هذه

الأنشطة بين تفتيش محتويات حقيبة ضابط مخابرات أمريكي أو الحصول على معلومات سرية تتعلق بخطط الولايات المتحدة المستقبلية لحلف الناتو. ورغم أن وكالة المخابرات المركزية الأمريكية نفت علنًا استخدام فخاخ العسل، إلا أن نظيرتها البريطانية، جهاز الاستخبارات البريطاني MI-6، استخدمت فخاخ العسل بانتظام خلال الحرب الباردة. وفي نادي إيف في شارع ريجنت بلندن، تم توظيف مجموعة نساء لإغراء الدبلوماسيين ورجال الأعمال السوفييت.

ولا تزال مصائد العسل التقليدية اليوم خيارًا قابلًا للتطبيق لجمع المعلومات الاستخباراتية، على الرغم من أن العديد من وكالات الاستخبارات لا تزال تنفي استخدام هذه الطريقة، فقد وُجهت اتهامات بالإيقاع الجنسي لأجهزة المخابرات الصينية.

الاستخبارات الإيرانية: من الثورة السياسية إلى الثورة الرقمية

رغم أن الجماعات غير المدعومة من الدولة يمكنها تشكيل وكالات استخبارات فضفاضة، إلا أنه قد يكون من الصعب بناء بيروقراطية استخباراتية فعالة دون دعم من

حكومة وطنية. عندما تكون الحكومات في حالة اضطراب، غالبًا ما يتعين على أجهزة الاستخبارات اتخاذ خيارات صعبة للغاية بهدف الحفاظ على الذات.

بعد سنوات من الاضطرابات السياسية وتوحيد مختلف الوكالات الحكومية، تم إنشاء وزارة الاستخبارات والأمن الإيرانية في أغسطس 1983 من أجل وضع أولويات استخباراتية جديدة وتبسيط مجتمع الاستخبارات الإيراني المنقسم.

بعد تشكيلها الأولي، كُلفت وزارة الاستخبارات الإيرانية بجمع المعلومات الاستخباراتية عن أعداء إيران الخارجيين والداخليين وتنفيذ مهام سرية مختلفة لدعم النظام الإيراني. واليوم، يعمل الحرس الثوري الإيراني (المسؤول عن الاستخبارات العسكرية) وفيلق القدس (المسؤول عن جمع المعلومات الاستخباراتية في الخارج) أيضًا كوكالات استخبارات تكميلية تعمل بالتنسيق مع وزارة الاستخبارات.

يُعرف الحرس الثوري الإيراني أيضًا بدعمه لمنظمات عميلة أجنبية عبر فيلق القدس. وتعمل هذه المنظمات العميلة الأجنبية كوكلاء لتنفيذ عمليات خارجية وتوسيع النفوذ الإيراني في منطقة الشرق الأوسط.

فيما يتعلق بعملياتها الاستخباراتية البشرية، فإن تركيز إيران ينصب إلى حد كبير على الولايات المتحدة والدول المجاورة لها.

على غرار العديد من أجهزة الاستخبارات الأخرى، تستخدم إيران غطاءً دبلوماسيًا لكثير من ضباطها. كما عُرفت إيران أيضًا بعدم دقتها في أساليبها الاستخباراتية، حيث انكشفت هوية العديد من دبلوماسييها على مر السنين. ومؤخرًا، وجهت إيران أيضًا عملياتها الاستخباراتية البشرية نحو أمريكا اللاتينية، حيث تستغل شبكات من الأفراد الشيعة للإبلاغ عن المصالح الإيرانية في نصف الكرة الجنوبي.

وبصرف النظر عن عملياتها الاستخباراتية البشرية، تعمل إيران ببطء على بناء قدراتها السيبرانية ليس فقط داخل مؤسساتها العسكرية، لكن أيضًا داخل كوادرها الاستخباراتية. ويمكن إرجاع الدافع وراء ذلك إلى عام 2010، عندما هز فيروس ستوكسنت إيران أجهزة الطرد المركزي.

وهذا دفع إيران إلى تخصيص تمويل حكومي لإنشاء مجلس أعلى للفضاء الإلكتروني. ومن شأنها في النهاية أن تنسق جميع برامج إيران الإلكترونية، وتعزز دفاعاتها

الوطنية، وتكمل جهودها في جمع المعلومات الاستخباراتية. وفي العام نفسه، أنشأت إيران أيضًا قيادة الدفاع السيبراني التي كُلفت بالدفاع عن البنية التحتية الحيوية الإيرانية. ومنذ عام 2010، دأبت إيران على تعزيز مواردها الإلكترونية بشكل مستمر.

والجانب الأكثر أهمية في برنامج إيران السيبراني لأغراض هو تجاوزه المجال التقليدي لعمليات الاستخبارات البشرية. مع تزايد تحليل عمليات الاستخبارات الإيرانية وإخضاعها للتدقيق العام، يتضح أن إيران تُظهر تفضيلًا متزايدًا للجمع بين الأدوات السيبرانية الحديثة وتقنيات محددة من أساليب الاستخبارات البشرية التقليدية.

ورغم أن النشاط الإلكتروني الخبيث لإيران قد شوهد في حملات البريد الإلكتروني الخبيثة واستغلال شبكات الكمبيوتر، إلا أنه أصبح أكثر انتشارًا داخل منصة وسائل التواصل الاجتماعي التي تتمحور حول الإنسان.

خداع الهوية ووسائل التواصل الاجتماعي

الخداع، كما هو مُعرّف في نظرية الخداع بين الأشخاص لبولر وبولجون ، هو "رسالة يرسها المرسل عن

علم لتعزيز اعتقاد أو استنتاج خاطئ لدى المتلقي". وفي السياق الرقمي، ظهرت نظريات عديدة لتفسير كيفية استمرار الخداع، وبخاصة خداع الهوية، في وسائل التواصل الاجتماعي.

وقد سلطت دراسات عديدة الضوء على خداع الهوية عبر الإنترنت ودور التحيز نحو الحقيقة وتأثير الهالة كمساهمين في نجاحه. إن التحيز نحو الحقيقة هو افتراض أن الجميع يقولون الحقيقة. ويؤدي هذا التحيز إلى تقليل قدرة مستخدمي وسائل التواصل الاجتماعي على اكتشاف متى يكذب شخص ما بشأن هويته.

ينبع تأثير الهالة من علم النفس الكلاسيكي ويتضمن تكوين أحكام إيجابية حول الأفراد بناءً على الانطباعات الأولى الإيجابية. وفي إحدى الدراسات، أدى انتهاك الفرد المبكر لمعيار اجتماعي قوي إلى تشويه النظرة الإيجابية للمجموعة تجاهه، رغم تصرفات الفرد المؤيدة للمجتمع والملتزمة بالمعايير بعد انتهاكه الأولي.

بالإضافة إلى التحيز نحو الحقيقة وتأثير الهالة، فإن التحرر الاجتماعي ظاهرة أخرى مرتبطة بالبيئات الرقمية والتي تمت مناقشتها في أدبيات علم النفس السيبراني.

وقد أطلق الباحث جون سولر على هذا التأثير اسم "تأثير التحرر من القيود عبر الإنترنت"، ويعتقد أن هذا التأثير مدعوم بعدة مكونات من التفاعل الرقمي بين الأشخاص. وسولر تحدث عن 6 عوامل تتفاعل وتساهم في تأثير التحرر من القيود عبر الإنترنت.

3 من العوامل الرئيسة تشمل:

- الإخفاء الانفصالي.
- العجز عن الرؤية
- ما يسميه سولر " عدم التزامن التواصلي ".

والأبحاث المبكرة حول التواصل عبر الحاسوب تشير إلى أن الناس أكثر كشفًا عن أنفسهم في البيئات الرقمية مقارنة بالتواصل وجهًا لوجه. وميز العلماء عمومًا بين نوعين من الخداع؛ أحدهما يتعلق بمقدمي المعلومات، والآخر يتعلق بطبيعة المعلومات المقدمة.

في حين أن العديد من الباحثين المعاصرين قد درسوا النوع الأخير من الخداع من خلال فحص ميل مستخدمي وسائل التواصل الاجتماعي إلى نقل المعلومات الخادعة، إلا أن عددًا أقل من الباحثين قد بحث في كيفية تأثير وسائل التواصل الاجتماعي على الطريقة التي يتم بها تنفيذ خداع الهوية.

باحثون عديدون قارنوا وسائل الإعلام المختلفة فيما يتصل بمعدلات الخداع (مقارنة الاتصالات الهاتفية والبريد الإلكتروني والرسائل الفورية بالتفاعلات وجهًا لوجه). ويصعب اكتشاف كل من الحقيقة والخداع في التواصل عبر الحاسوب قياسًا بالتفاعلات وجهًا لوجه، وذلك بسبب نقص الإشارات المادية والبصرية للمصدر.

هذا الأمر يترك مستخدمي التواصل عبر الحاسوب في الغالب أمام مهمة تفسير الإشارات النصية والمحتوى. بالإضافة إلى ذلك، وجد الباحثون أن أنواع الأكاذيب التي يرويها الناس في التفاعلات المباشرة تختلف عن أنواع الأكاذيب التي تُروى في التواصل عبر الحاسوب.

ففي التفاعلات وجهًا لوجه، يكذب الناس أكثر عن طريق الإغفال، بينما في التواصل عبر الحاسوب، يكذبون أكثر عن طريق الفعل (أي الكذب الصريح). وتتضمن بعض الأساليب المحددة المستخدمة لإدامة الخداع في وسائل التواصل الاجتماعي "الخداع، والتقليد (مثل تقليد موقع ويب)، والتزييف (مثل إنشاء موقع ويب مزيف)، والأكاذيب البيضاء، والتهرب، والمبالغة، وإعادة توجيه صفحات الويب (مثل تضليل شخص ما إلى صفحة ملف

تعريف مزيفة)، والإخفاء (مثل حجب المعلومات من ملف تعريف الشخص)".

ركزت الأبحاث المتعلقة بالكشف عن خداع الهوية في وسائل التواصل الاجتماعي بشكل كبير على الوسائل الآلية أو التقنية للكشف عن الخداع. من خلال استخدام الذكاء الاصطناعي والتعلم الآلي، يقوم العديد من الباحثين باستكشاف إمكانيات التحليل النصي في الكشف عن الهويات المزيفة. ومن خلال استخدام نماذج التعلم الخاضعة للإشراف، سعى بعض الباحثين إلى كشف الهويات المزيفة من خلال تحليل الرسائل النصية على وسائل التواصل الاجتماعي.

وفي بعض الدراسات، طُبِّق الذكاء الاصطناعي على الهوية المزيفة وقد أثبت الكشف أن نسبة نجاحه تصل إلى 99 بالمائة. ومع ذلك، فإن الغالبية العظمى من هذا البحث كانت تتعلق بالبريد العشوائي أو الحسابات التي تم إنشاؤها بواسطة برامج الروبوت وليس بالحسابات التي يتم تشغيلها يدويًا بواسطة البشر الذين يدّعون أنهم بشر آخرون.

مع ازدياد مشاركة البشر في وسائل التواصل الاجتماعي، تميل المشاعر العالمية للثقة والأمل والقبول

الاجتماعي إلى التأثير على الحكم النقدي وتؤدي إلى انخفاض معدلات اكتشاف الخداع بشكل كبير. وخارج نطاق الواجهات الرقمية، يُعرف عن البشر أنهم سيئون للغاية في اكتشاف الخداع بين الأشخاص، حيث تكون معدلات الكشف أفضل بقليل من الصدفة العشوائية أو دقة 50 بالمائة.

وتتضاعف مخاطر الخداع، حيث يمكن إنشاء شخصيات رقمية بسرعة عبر العديد من منصات التواصل الاجتماعي. رغم قلة الأبحاث التي تستخدم البالغين، فقد استخدم الباحثون الرقميون الأطفال بموافقة الوالدين في دراسات خداع الهوية الخاضعة للرقابة.

في إحدى الدراسات، طُلب من الأطفال الذين تتراوح أعمارهم بين 12 و 18 عامًا تحديد عمر شخص غريب في غرفة دردشة وجنسه. وكانت النتائج الرئيسة في هذه الدراسة أن:

- 16% فقط من الأطفال المشاركين كانوا على صواب في تخمين العمر.
- 10% فقط كانوا على صواب في تخمين الجنس.

رغم زيادة معدلات الكشف بين الأشخاص الأكبر سنًا، إلا أن أعلى معدلات الكشف كانت 22 بالمائة

(لتخمين العمر) و 16 بالمائة (لتخمين الجنس) بين طلاب الصف الحادي عشر وطلاب الصف الثاني عشر.

عندما سُئل الأطفال المشاركون عن كيفية تقييمهم لمدى صحة هويات المستخدمين عبر الإنترنت، قالوا إن المحتوى (مثل ما تحدث عنه المستخدم) لعب دورًا رئيسًا في عملية اتخاذ القرار لديهم.

التصيد الاحتيالي الموجه

يُعدّ التصيد الاحتيالي الموجه أحد الأشكال المحددة بشكل خاص للخداع في الهوية عبر الإنترنت. رغم أن التصيد الاحتيالي الموجه يتخذ أشكالًا وأنواعًا عديدة، إلا أن ستيفن نورثكوت من معهد SANS للتكنولوجيا يعرفه بأنه: "هجوم دقيق ضد مجموعة فرعية من الأشخاص (مستخدمي موقع ويب أو منتج، أو موظفي شركة، أو أعضاء منظمة) في محاولة لتقويض تلك الشركة أو المنظمة".

ويستهدف هذا النوع من الهجمات الإلكترونية فئة محددة من الأشخاص، بدلًا من إرسال رسائل عشوائية إلى الجميع، ويحاول حثهم على القيام بشيء ما للوصول إلى بيانات سرية أو أنظمة الشركة. غالبًا تبدو هذه الرسائل

حقيقية وكأنها صادرة من عضو رسمي في المؤسسة. على سبيل المثال، قد تبدو رسالة التصيد الاحتيالي الموجهة وكأنها صادرة من أحد المديرين التنفيذيين في الشركة يطلب فيها أسماء مستخدمين وكلمات مرور.

على غرار رسائل البريد الإلكتروني العشوائية، فإنّ فعل التصيّد الاحتيالي الخبيث (أي استهداف العديد من الأفراد بهدف الوصول إلى معلومات حساسة) موجود منذ بدايات الإنترنت. أما التصيّد الموجّه، فهو أحدث عهدًا. وعلى عكس التصيد الاحتيالي العام، يتطلب التصيد الاحتيالي الموجه مزيدًا من الوقت والجهد، لكنه قد يحمل حمولات أكبر.

مع مرور الوقت، أدرك كل من المجرمين الصغار والدول فعالية التصيد الاحتيالي الموجه في الحصول على الأموال ومواد الابتزاز والمعلومات السرية. رغم أن البريد الإلكتروني لا يزال الطريقة المفضلة للتصيد الاحتيالي الموجه في جميع أنحاء العالم، إلا أن استخدام وسائل التواصل الاجتماعي كمنصة للتصيد الاحتيالي الموجه يكتسب زخمًا.

في أغسطس 2018، أعلن مسؤول استخباراتي أمريكي علنًا أن الصين تشن حملة "عدوانية للغاية"

لاستهداف مستخدمي LinkedIn الذين لديهم إمكانية الوصول إلى مواد سرية. قبل ذلك بعام، نُشِرَت إفادة خطية غير مختومة، تفصل عملية التوظيف عبر الإنترنت لحامل تصريح أمني سري للغاية سابق، كيفن مالوري. تكشف الإفادة الخطية أن مالوري تم الاتصال به عبر موقع لينكد إن من قبل شخص اعتقد أنه صائد رؤوس صيني.

بعد تبادل الرسائل ذهابًا وإيابًا، سافر مالوري في النهاية إلى الصين وأحضر معه العديد من وثائق الحكومة الأمريكية المصنفة على أنها سرية للغاية. ووجه مكتب التحقيقات الفيدرالي لائحة اتهام إلى مالوري بتهمة واحدة بموجب المادة 8 من قانون الولايات المتحدة § 1001 (تقديم بيانات كاذبة جوهرية) وتهمة واحدة بموجب المادة 18 من قانون الولايات المتحدة § 794 (جمع أو تسليم معلومات دفاعية لمساعدة حكومة أجنبية).

على غرار حملة التدخل الروسي في الانتخابات، فإن جهود التصيد الاحتيالي الصينية على موقع لينكد إن ليست سوى جزء صغير من نشاط الاستخبارات الأجنبية اليوم داخل وسائل التواصل الاجتماعي. رغم استحالة الإلمام بجميع تفاصيل هذا العالم الرقمي المتنامي لجمع المعلومات الاستخباراتية، إلا أن التركيز على دولة واحدة

وتكتيك واحد يُعدّ مفيدًا لدراسة الاتجاهات واستشراف المستقبل. في هذا الفصل، سنتناول الخلفية والتحليل والتوصيات المتعلقة بدولة إيران ومفهوم "الفخاخ الرقمية."

المنهجية

كطريقة لتحليل كيفية استخدام الجماعات الإلكترونية المدعومة من الدولة الإيرانية للفخاخ الرقمية في وسائل التواصل الاجتماعي، سيتناول هذا الفصل حالتين حديثتين. تُقدّم طريقة دراسة الحالة شكلًا مثاليًا لفحص العمليات المعقدة وعزل الجوانب المهمة للمفاهيم النظرية.

الحالة الأولى التي ستتم دراستها بشخصية مزيفة على موقع لينكد إن تدعى "ميا آش"، ومجموعة إلكترونية إيرانية، والعديد من أعضاء لينكد إن غير المدركين الذين أصيبوا ببرامج تجسس بعد التفاعل مع شخصية جذابة، ولكنها في النهاية مزيفة. وتتضمن دراسة الحالة الثانية منشقًا أمريكيًا.

فيما يتعلق بمعايير اختيار الحالات، كانت السمات التالية من أسباب اختيار الحالات: ثراء البيانات،

ونموذجية ظروف خلفية الحالة، والأهمية الجوهرية. اختيرت هذه الحالات نظرًا لتغطيتها العالية نسبيًا في الخطاب الدولي للأمن السيبراني والتقارير الصحفية. ورغم أن حالات أخرى من التجسس الإلكتروني والهجمات الإلكترونية تمت تغطيتها في وسائل الإعلام العامة، إلا أن العديد من هذه الحالات الأخرى تفتقر إلى تحليل متعمق للتكتيكات والتقنيات والإجراءات المستخدمة، فضلًا عن التقارير المؤيدة، وهذا سبب عدم اختيارها.

اختيرت هذه الحالات لاستخدامها المتعمد لفخ العسل الرقمي في سياق وسائل التواصل الاجتماعي، ولأهميتها الجوهرية ومدى صلتها بمجالات الاهتمام السياسي الحالية البالغ عددها 63 مجالًا. لطالما كان التدخل الاستخباراتي الأجنبي عبر وسائل التواصل الاجتماعي موضوع نقاش مطول داخل الهيئة التشريعية الأمريكية وأولوية عالية لمجتمع الاستخبارات الأمريكي منذ الانتخابات الرئاسية لعام 2016.

ولأن فخ العسل الرقمي يمثل تهديدًا استخباراتيًا أجنبيًا متطورًا في مجال النشاط السري الرقمي، فإن دراسة العديد من الحالات الحديثة ستوفر فائدة جوهرية لصناع السياسات والمواطنين الأمريكيين.

دراسة حالة رقم 1: ميا آش، منصة النفط، وبابي رات

SecureWorks التابعة لشركة Dell اكتشفت بعض أنشطة إلكترونية خبيثة تشبه التكتيكات والتقنيات والإجراءات التي تستخدمها مجموعة تهديد إلكتروني إيرانية معروفة باسم: OilRig. ثم في عام 2017، ظهر ملف تعريف على موقع لينكد إن يعود لامرأة باسم المستخدم ميا آش. بدأ الملف الشخصي بإرسال دعوات للتواصل مع مجموعة مختارة من الرجال عبر الإنترنت.

ادعى آش أنه مصور في العشرينات من عمره مقيم في لندن، وأظهر انجذابًا خاصًا للرجال الشرق أوسطيين الملمين بالتكنولوجيا الذين يعملون في صناعات تكرير النفط والغاز. وللحفاظ على مظهرها الرقمي، كان لدى آش سيرة ذاتية تبدو شرعية، والعديد من صور الملف الشخصي المُفلترة، بالإضافة إلى منشورات وتحديثات منتظمة على حساباتها على وسائل التواصل الاجتماعي. بالنسبة لمستخدم لينكد إن غير المتكلف، بدا ملف آش الشخصي الذي يحتوي على أكثر من 500 جهة اتصال

متواضعًا، إن لم يكن ذا علاقات واسعة، وذلك بالنظر إلى المظهر المصقول لملفها الشخصي.

بالإضافة إلى ملفها الشخصي القوي على لينكد إن، كان لدى آش أيضًا حسابات على مواقع التواصل الاجتماعي مثل: فيسبوك، وبلوجر، وواتساب، وموقع التواصل الاجتماعي الفني على الإنترنت، ديفيانت آرت. ظاهريًا، بدت آش كشابة ودودة ومغامرة ولديها ميل إلى المديرين التنفيذيين رفيعي المستوى في الشرق الأوسط في صناعات تكرير النفط والتكنولوجيا.

كانت طريقة عملها بسيطة. كانت آش تبدأ الاتصال عن طريق إرسال رسالة بريئة إلى الرئيس التنفيذي أو نائب الرئيس عبر تطبيق المراسلة الخاص بـ LinkedIn، ثم تطلب من صديقها الجديد نقل مراسلاتهم إلى منصة تواصل اجتماعي مختلفة، عادةً تكون Facebook أو Messenger أو مزود خدمة بريد إلكتروني.

بينما كانت آش تستدرج أهدافًا ذات قيمة عالية عبر وسائل التواصل الاجتماعي، في حوالي فبراير 2017، رصدت شركة ديل سكيور بعض الأنشطة الإلكترونية الخبيثة الإضافية التي تشبه التكتيكات والتقنيات

والإجراءات التي تستخدمها مجموعة التهديد الإلكتروني الإيرانية المعروفة باسم: OilRig.

ويبدو أن مجموعة كبيرة من أجهزة الكمبيوتر التابعة للشركات تعرضت للاختراق عبر وحدات ماكرو خبيثة مضمنة في جداول بيانات مايكروسوفت إكسل أُرسِلَت عبر مرفقات البريد الإلكتروني. واكتُشِف أن أحد موظفي شركة في الشرق الأوسط كان يتواصل مع شخصية ميا آش على لينكد إن لأكثر من شهر.

وبحسب إفادات الضحايا، بدأ أحد موظفي الشركة المتضررة علاقة عبر الإنترنت مع آش على موقع لينكد إن. توجهت آش إلى الموظف بأسئلة تتعلق بالتصوير الفوتوغرافي، ثم انتقلت العلاقة إلى فيسبوك ومواقع أخرى للتواصل الإلكتروني. في إحدى مراحل اتصالاتهما، طلبت آش من الموظف تنزيل "استبيان التصوير الفوتوغرافي"، على شكل جدول بيانات مايكروسوفت إكسل.

علاوة على ذلك، أصرّت آش على أن يفتح الموظف الاستبيان على جهاز الكمبيوتر الخاص بالعمل، وإلا، كما أخبرته، لن يعمل الاستبيان بشكل صحيح. لسوء الحظ، بمجرد فتح الملف، أطلق الموظف برنامجًا خبيثًا للتحكم عن بُعد (RAT) يحصل على الفور على صلاحيات

المسؤول في جميع أنحاء شبكة الكمبيوتر الخاصة بالشركة ويبدأ في تسريب سجلات رقمية حساسة إلى خادم بعيد.

بعد أشهر من تحليل نشاط البرنامج وإجراء التحليل الجنائي الإلكتروني، عزت شركة SecureWorks برنامج التجسس عن بعد إلى ميا آش، وتاليًا إلى مجموعة التهديد المستمر المتقدمة الإيرانية: OilRig

دراسة حالة رقم 2: شبكة فيسبوك السرية لبيلا وود

قُدِّمَت لائحة اتهام من 7 تهم ضد العميلة الخاصة السابقة في مكتب التحقيقات الخاصة التابع للقوات الجوية مونيكا ويت في مقاطعة كولومبيا. بالإضافة إلى الكشف عن سلسلة من تهم التجسس الموجهة ضد ويت، كشفت لائحة الاتهام التي تم رفع السرية عنها أيضًا عن حملة فخ رقمية غير معروفة سابقًا استهدفت موظفين القوات الجوية الأمريكية لديهم إمكانية الوصول إلى برامج متخصصة.

وشملت الأهداف "العملاء الخاصين الحاليين أو السابقين، ومحللي مكافحة التجسس، وغيرهم من

موظفي لجنة الاستخبارات الأمريكية الذين كانوا زملاء عمل" لويت.

بدأت قصة انشقاق ويت في نهاية المطاف إلى إيران قبل سنوات من اتهامها بانتهاكا القانون الأمريكي. ففي فبراير 2012، سافرت ويت إلى إيران لحضور مؤتمر "الهوليوودية"، الذي رعاه الحرس الثوري الإيراني بهدف إدانة المعايير الأخلاقية المتساهلة في أمريكا. وبعد ذلك بوقت قصير، ظهرت ويت في مقاطع فيديو على الإنترنت، حيث صرّحت علنًا بكونها جندية أمريكية سابقة، وآرائها المعادية لأمريكا، وأعلنت اعتناقها الإسلام مؤخرًا.

استنادًا إلى أدلة القضية، صرح مسؤولو مكتب التحقيقات الفيدرالي لاحقًا بأن انشقاق ويت يبدو أنه ذو طبيعة أيديولوجية. فبين عامي 2012 و 2013، كانت ويت على اتصال بالحرس الثوري الإيراني وشخص تم تحديده باسم "الشخص أ" في لائحة الاتهام. من خلال مقتطفات من اتصالات جمعها مكتب التحقيقات الفيدرالي، بدت ويت حريصة على مساعدة إيران، وقد أُتيحت له في نهاية المطاف عدة فرص للقيام بذلك، إلى حد كبير من خلال وسائل التواصل الاجتماعي.

في حوالي شهري يوليو وأغسطس 2013، بدأت ويت بإجراء عمليات بحث على فيسبوك عن زملاء سابقين في مكافحة التجسس في مكتب التحقيقات الخاصة التابع للقوات الجوية الأمريكية. وفي 28 أغسطس 2013، انشقت ويت رسميًا وسافرت إلى إيران، ومنذ ذلك الحين، أجرت حوارات على فيسبوك مع موظفي الحكومة الأمريكية باستخدام حسابات فيسبوك وهمية مسجلة لهويات مزيفة متعددة.

بين يناير 2014 ومايو 2015، أنشأت ويت "حزم أهداف" لاستخدامها من قبل إيران ضد عملاء الحكومة الأمريكية، وضمن ذلك ضباط مكافحة التجسس التابعين لمركز الاستخبارات الأمريكي."

علاوة على ذلك، وفي الوقت نفسه تقريبًا، كشفت ويت عن الاسم الحقيقي لعميل حكومي أمريكي، بالإضافة إلى حقيقة أنها قامت بأنشطة مكافحة التجسس، وبينما كانت تقوم بأبحاث الهندسة الاجتماعية وتبني حزم استهداف مستمدة من وسائل التواصل الاجتماعي، في 5 يناير 2015، أنشأت مجموعة فاعلين إلكترونيين إيرانيين حساب بريد إلكتروني: bella.wood87@yahoo.com بالإضافة إلى حساب فيسبوك مرتبط باسم المستخدم: Bella Wood

واستخدمه الفاعلون الإلكترونيون الإيرانيون لإرسال طلب صداقة على فيسبوك إلى موظف حكومي أمريكي (يشار إليه في لائحة الاتهام باسم "عميل الحكومة الأمريكية 2") كان آنذاك في العاصمة الأفغانية كابول مع وحدة استخبارات تابعة للقيادة المركزية الأمريكية (CENTCOM).

وخلال هذه المهمة، استخدم العميل الأمريكي رقم 2 جهاز كمبيوتر تابعًا لوزارة الدفاع الأمريكية للوصول إلى موقع فيسبوك. وفي حوالي 9 يناير 2015، وأرسل عدد من المتسللين الإلكترونيين الإيرانيين بريدًا إلكترونيًا إلى العميل الأمريكي رقم 2 يحتوي على رابط مزيف يُزعم أنه يُوجه العميل إلى "بطاقة جميلة". والرابط المزيف كان في الواقع يؤدي إلى خادم يتم التحكم فيه من قبل جهات فاعلة إلكترونية إيرانية.

كما استخدمت الرسالة الإلكترونية نفسها برامج تتبع سرية للتأكد من أن العميل الأمريكي رقم 2 كان يقرأ الرسالة الإلكترونية من شبكة حاسوب تابعة لوزارة الدفاع الأمريكية موجودة في كابول، أفغانستان.

في 9 يناير 2015، أرسلت bella.wood87@yahoo.com بريدًا إلكترونيًا إلى العميل رقم 2 التابع للحكومة الأمريكية مرة أخرى، باستخدام النص التالي:

سأرسل لكِ ملفًا يحتوي على صوري، لكن عليكِ تعطيل برنامج مكافحة الفيروسات لفتحه. ويجب فتحها على جهاز الكمبيوتر الخاص بكِ. وكان من المفترض أن تؤدي الروابط إلى الصور المزعومة إلى توجيه العميل الأمريكي رقم 2 إلى خادم تسيطر عليه جهات فاعلة إلكترونية إيرانية.

في الفترة الزمنية نفسها تقريبًا، أنشأ فاعلون إلكترونيون إيرانيون حسابًا مزيفًا على فيسبوك باستخدام الاسم الحقيقي لشخص ورد ذكره في لائحة الاتهام باسم "عميل الحكومة الأمريكية رقم 3". تم ذلك باستخدام صور حقيقية ومعلومات جُمعت من حساب فيسبوك شرعي يديره العميل الأمريكي رقم 3.

وباستخدام حسابهم المزيف الجديد على فيسبوك، أرسل الفاعلون الإلكترونيون الإيرانيون طلب صداقة على فيسبوك إلى شخص يُعرف باسم عميل الحكومة الأمريكية رقم 1، والذي قبله.

في غضون 24 ساعة تقريبًا، أرسل حساب فيسبوك مزيف رسالة إلى العميل الأمريكي رقم 1 تحتوي على ما يبدو أنه ملف صورة بصيغة jpg. ، لكنه في الواقع كان ملفًا مضغوطًا بصيغة zip. يحتوي على برامج ضارة من شأنها أن تمنح الجهات الفاعلة الإلكترونية الإيرانية "وصولًا سريًا ومستمرًا إلى جهاز الكمبيوتر الخاص بالعميل الأمريكي رقم 1 وأية شبكة مرتبطة به".

في حوالي 10 مارس 2015، تمكن قراصنة إيرانيون من إقناع مستخدم على فيسبوك يُعرف باسم "عميل الحكومة الأمريكية رقم 5" ليس فقط بقبول طلب صداقة، بل أيضًا بتزكية حساب فيسبوك مزيف وإضافته إلى مجموعة خاصة على فيسبوك تضم في معظمها عملاء للحكومة الأمريكية. وبذلك، تمكن القراصنة الإيرانيون من الوصول إلى معلومات شخصية وحساسة تخص موظفي الحكومة الأمريكية.

في مايو 2015، أرسل الحساب المزيف نفسه رسائل منفصلة إلى 4 موظفين آخرين في الحكومة الأمريكية تحتوي على روابط بدت وكأنها تؤدي إلى مقالات إخبارية دولية، لكنها في الواقع كانت تؤدي إلى صفحات تسيطر عليها جهات فاعلة إيرانية في مجال الإنترنت.

ورغم أن الجمهور لن يعرف على الأرجح المدى الكامل للضرر الذي تسببت فيه ويت، فقد وصفه مسؤولون استخباراتيون سابقون بأنه "شديد"، نظرًا لتصريح ويت الأمني السري للغاية السابق، وانتهاكاتها لقوانين الدفاع الوطني، والشكوك في أنها كشفت عن أسماء عملاء مزدوجين تديرهم الولايات المتحدة.

تحليل دراسة الحالة

في التجسس الكلاسيكي، يكون "صائدو العسل" رجالًا ونساءً يجري إعدادهم لجذب انتباه أهداف استخباراتية غير متوقعة، لكن في حالة "السنونو" التابعين لـ (كي. جي. بي.)، وأحيانًا كان يتم ابتزاز هؤلاء الذين يعملون "صائدي عسل" للعمل كعملاء للدولة. وغالبًا خلقت هذه الديناميكية القائمة على التعامل القسري مشاكل لعناصر (كي. جي. بي.) الذين يتعاملون مع طيور السنونو.

وفي العالم الرقمي، حيث لا تعد الفخاخ سوى شفرة حاسوبية، لا يمتلك المشغلون الإيرانيون سيطرة أكبر على "ضحاياهم" الرقميين فحسب، ويواجهون مخاطر أقل بكثير للانشقاق، بل يمتلكون أيضًا ثروة معرفة عالمية تكون في متناول أيديهم.

قد تكون هذه بعض الأسباب التي دفعت إلى استخدام شخصية ميا آش المزيفة وتُعتبر واحدة من أكثر الشخصيات تطورًا في مجال "فخ العسل" في التاريخ الحديث.

ومع ذلك، وعلى الرغم من نجاحاتها، لم تكن آش مثالية. وكما هو الحال مع العديد من حسابات التواصل الاجتماعي المزيفة، فإن المحتوى الرقمي الذي شكّل ملف آش لم ينشئه ضباط المخابرات الإيرانية، بل سُرِق من مواقع مختلفة على الإنترنت.

بدلًا من أن تكون كيانًا مستقلًا، كانت شخصية ميا آش عبارة عن مزيج رقمي من ملفات JPEG وملفات نصية عادية متاحة للجمهور والتي سُرقت من الحياة الرقمية للآخرين.

سُرِق العديد من صور الملف الشخصي الخاصة بـ Ash والصور التي تم تحميلها على حسابها في Blogger من امرأة رومانية تحمل اسم المستخدم: Bittersweetvenom على موقع DeviantArt . 234 ، بالإضافة إلى ذلك، يبدو أن النقاط الرئيسة في سيرة آش الذاتية على موقع لينكد إن نُسِخت حرفيًا تقريبًا من ملف تعريف امرأة أمريكية على لينكد إن.

من وجهة نظر الملكية الفكرية، كانت شخصية آش بأكملها انتهاكًا ضخمًا لقانون حقوق النشر، وهو ما لم يكتشفه أحد حتى أدرك ضحاياها الضرر الجسيم الذي ألحقته بالأمن القومي. وكجزء من تحليلهم المنشور، شركة سكيور لاحظ باحثو الأعمال العديد من الشذوذات المحددة في الشبكات الاجتماعية، والتي ساعدتهم في نسب شخصية ميا آش إلى جماعة التهديد الإيرانية.

أولًا، كانت جميع علاقات آش غير المتعلقة بالتصوير الفوتوغرافي توجد مع شركات في: بنغلاديش والهند والعراق وإيران وإسرائيل والسعودية والولايات المتحدة، وجميعها تعمل في مجالات التكنولوجيا والنفط والغاز، والرعاية الصحية، والفضاء، والاستشارات.

كان هذا الحشد من أهداف الاستخبارات الإيرانية، الذي شكّل الجزء الأكبر من علاقات آش، أحد المؤشرات الأولى لشركة سكيور وركس على أن ميا آش لديها دوافع خفية.

ثانيًا، جميع معارف آش كانوا "موظفين من المستوى المتوسط في الأدوار التقنية (الميكانيكية والحاسوبية) أو إدارة المشاريع بمسميات وظيفية مثل مهندس الدعم الفني ومطور البرامج ودعم النظام".

وبالنسبة لمحلل الأمن السيبراني المدرب، كان الأشخاص الذين يشغلون هذه الأدوار يتمتعون بصلاحيات وصول مرتفعة داخل شبكات الشركات، ما كان سيمنح جهة تهديد سيبراني وصولًا أفضل إلى البيئة المستهدفة.

ثالثًا، يبدو أن جميع علاقات آش تتوافق مع أهداف الحكومة الإيرانية الأوسع نطاقًا "الأيديولوجية والسياسية والاستخباراتية العسكرية". وبغض النظر عن مؤشرات تورط المخابرات الإيرانية في شخصية آش، فإن شبكة التواصل الاجتماعي المزيفة المتطورة التي ساعدتها معرفة وبحث المنشقة مونيكا ويت تُظهر تصعيدًا خطيرًا لعمليات المخابرات الإيرانية في وسائل التواصل الاجتماعي.

رغم أن لائحة الاتهام الموجهة ضد ويت تتجنب تسمية أفراد معينين أو الخوض في تفاصيل كثيرة حول محتوى الاتصالات بين شخصيات ويت المزيفة وأهدافها، إلا أنها توضح مدى سهولة اختراق ويت لشبكة غير مدركة من الزملاء السابقين وعملاء الحكومة الأمريكية الحاليين.

على غرار شخصية آش، استخدمت ويت صورًا من صفحة شخص آخر على وسائل التواصل الاجتماعي، لكن ويت كانت تتمتع بميزة القدرة على الاستفادة من معرفتها الشخصية بالأهداف. وسمح لها ذلك بصياغة محتوى ورسائل غير مثيرة للقلق، ما مكنها من الحصول على ردود إيجابية على طلبات "الصداقة" السرية التي كانت ترسلها. بالإضافة إلى ذلك، وباعتباره شخصًا لديه خبرة في استخدام منصة التواصل الاجتماعي فيسبوك والاستعلام عنها والتلاعب بها، كانت ويت مدربة جيدًا للتسلل إلى شبكاتها الاجتماعية المتباينة، وضمن ذلك مجموعة فيسبوك خاصة بموظفي الحكومة الأمريكية.

في لائحة الاتهام التي وجهها مكتب التحقيقات الفيدرالي إلى ويت، يفصّل عميل مكتب التحقيقات الفيدرالي جولات البحث المتعددة التي أجرتها في بوابة البحث المفتوحة لفيسبوك. كانت مهارات ويت البحثية وبناء العلاقات جيدة للغاية، لدرجة أنها تمكنت من اختراق مجموعة خاصة على فيسبوك، ما أتاح لها الوصول إلى مخزون من المعلومات ومجموعة مختارة مسبقًا من العملاء المحتملين.

بالمقارنة مع شخصية ميا آش، تُظهر حالة مونيكا ويت أنه رغم أن جمع المعلومات الاستخباراتية البشرية أصبح رقميًا بشكل متزايد، إلا أن الإدراج القيّم للعامل البشري من المرجح أن يجعل الفخاخ الرقمية أكثر تطورًا وفعالية، وبخاصة إذا كان هناك منشقون متحمسون مدفوعون أيديولوجيًا.

عندما تقوم وكالة استخبارات أجنبية بصياغة حملة تسويقية سرية بسيطة للتأثير في الجماهير، يمكن القضاء على الكثير من الملل باستخدام الذكاء الاصطناعي والخوارزميات المصممة بعناية والدعاية الحاسوبية، مع ذلك، عندما يتعلق الأمر باستهداف الأفراد ذوي القيمة العالية (مثل زملاء ويت السابقين في مكافحة التجسس في مكتب التحقيقات الخاصة التابع للقوات الجوية)، فإن قضية مونيكا ويت توضح ميزة وجود إنسان حي يتنفس على الجانب الآخر من الشاشة، ويمكنه التعامل مع الفروق الدقيقة لوسائل التواصل الاجتماعي وبث جو من المصداقية في الشخصيات الخبيثة على الإنترنت. ويُعتقد أن ويت تقيم اليوم في إيران، حيث تتمتع بحماية فعالة من تسليمها إلى الولايات المتحدة.

بغض النظر عن مكان إقامتها، تسمح وسائل التواصل الاجتماعي باستمرار لهذه الحاملة السابقة لتصريح أمني أمريكي بإلحاق ضرر أكبر بمصالح الأمن القومي الأمريكي ما كان بإمكانها فعله قبل ظهور وسائل التواصل الاجتماعي. من خلال ربطها بمشغليها وخبراء الأمن السيبراني الإيرانيين، تسمح وسائل التواصل الاجتماعي لعمليات الاحتيال الإلكتروني الموجهة عن بُعد، مثل عملية ويت، بالتصرف بتهور ودون رادع.

خاتمة

وفقًا لمؤشر استخبارات الأمن السيبراني لعام 2014 الصادر عن خدمات أمن IBM، فقد أقرت IBM بأن "الخطأ البشري" كان عاملًا مساهمًا في أكثر من 95 بالمائة من جميع الحوادث التي تم التحقيق فيها.

وفي مجال الاستخبارات الحديثة، حيث أدى الإنترنت إلى زيادة حجم سطح الهجوم العالمي بشكل كبير، يمكن أن تتحول الأخطاء البشرية الطفيفة في التقدير إلى كوارث لا رجعة فيها للأمن القومي. وأجهزة المخابرات الإيرانية تثبت أنها مبتكرة ودؤوبة في جهودها للوصول إلى المعلومات الحساسة. وتحت السطح اللامع

لوسائل التواصل الاجتماعي، من المهم أن نتذكر أن كل ما يتطلبه الأمر هو لحظة واحدة من الخطأ البشري لكي يتمكن الأعداء من الوصول إلى كنوز من المعلومات السرية للغاية.

ورغم أن الآثار الأولية لخداع الهوية قد تبدو غير مهمة، إلا أن التكاليف طويلة المدى لعمليات النصب الناجحة وغيرها من عمليات الاستخبارات الخبيثة يمكن أن تكون مدمرة. إن تسريب أسرار الدولة ونهب التقنيات الحساسة ليسا سوى بعض المكاسب الأولية التي تجنيها وكالات الاستخبارات الأجنبية من أنواع العمليات التي تم تحليلها في هذا الفصل.

مع ظهور تحديات جديدة وتطور تكتيكات الخصوم السيبرانيين الأجانب، يمكن أن يكشف البحث المستمر في هذا المجال عن النشاط الخبيث، ويربط الخيوط المشتركة التي تنسب الجهات الفاعلة السيبرانية السيئة، ويطور تدابير إضافية لمكافحة التجسس.

الفصل الثالث
الاستخبارات الصينية في وسائل التواصل الاجتماعي

سيتناول هذا الفصل كيف ساهمت وسائل التواصل الاجتماعي في تعزيز عملية تجنيد العملاء الصينيين. وتتميز الصين عن غيرها من خصوم أمريكا في مجال الاستخبارات الخارجية لأسباب عديدة. ومن المعروف أن المخابرات الصينية تجند عملاءها في المقام الأول من أصول صينية. ومن المعروف أيضًا أنها تتبنى وجهة نظر أوسع لما قد تسميه العديد من الوكالات الأخرى "الاستخبارات."

وأخيرًا، على عكس العديد من ضباط المخابرات الغربيين الذين يجعلون الأمر واضحًا عندما يقومون بتجنيد شخص ما ويدخلون في علاقة سرية، نادرًا ما يصنف الصينيون هذه العلاقات الاستخباراتية القيّمة على هذا النحو. بدلًا من ذلك، سيصنف ضباط المخابرات

الصينيون العلاقة على أنها اجتماعية أو مهنية، رغم أن هناك أبعادًا واضحة لجمع المعلومات الاستخباراتية بالنسبة للعيون الغربية المدربة تدريبًا عاليًا.

ومن أبرز جوانب الاستخبارات الصينية نهجها في جمع المعلومات، ويعتمد على "حبات الرمل" أو "الفراغ." ويوصف هذا النهج من خلال استعارة انتشرت عبر قسم مكافحة التجسس التابع لمكتب التحقيقات الفيدرالي لسنوات وأصبحت مرادفة للخصم الاستخباراتي الآسيوي الأول لأمريكا. كما أوضح المحلل السابق في مكتب التحقيقات الفيدرالي بول مور: "إذا كان الشاطئ هدفًا للتجسس، فإن

- الروس سيرسلون غواصة، وسيتسلل الغواصون إلى الشاطئ في ظلام الليل، وبسرية تامة يجمعون عدة دلاء من الرمل ويعيدونها إلى موسكو."
- ستستهدف الولايات المتحدة الشاطئ بالأقمار الصناعية وتجمع كميات هائلة من البيانات.
- الصينيون سيرسلون ألف سائح، يُكلف كل منهم بجمع حبة رمل واحدة. وعند عودتهم، سيُطلب منهم نفض مناشفهم. وسينتهي بهم الأمر بمعرفة المزيد عن الرمال أكثر من أي شخص آخر.

يُعدّ هذا النهج الدقيق والحذر للغاية في مجال الاستخبارات أحد أبرز سمات الاستخبارات البشرية الصينية. أما فيما يتعلق بفعاليته، فقد كان هذا الأمر محل نقاش تاريخي. ولعقود من الزمن، كان من غير الواقعي معالجة وفرز وفهم هذه الكميات الكبيرة من المعلومات.

اليوم، ومع ظهور التعلم الآلي والحواسيب العملاقة والذكاء الاصطناعي، أصبحت تقنية جمع المعلومات التي كانت تعتبر في السابق مفرطة وغير فعالة من قبل وكالات الاستخبارات الأخرى، واقعًا مثمرًا. ومع تحول سجلات الصين وبقية العالم إلى سجلات رقمية، يقترب مجال الاستخبارات دلاليًا من تجسيد استعارة حبات الرمل.

لا يوجد مكان يتجلى فيه هذا الأمر أكثر من عالم وسائل التواصل الاجتماعي. وبينما فضلت الصين تاريخيًا رصد وتقييم وتجنيد ومقابلة عملائها الاستخباراتيين على الأراضي الصينية، فقد وفر القرن 21 وسيلة إضافية لتجنيد العملاء البشريين في شكل وسائل التواصل الاجتماعي.

في البيئة الرقمية لوسائل التواصل الاجتماعي، تزدهر العلاقات السرية، وتصبح الاتصالات المشفرة هي القاعدة، ولا يوجد مسؤولون جمركيون افتراضيون للاستفسار عما إذا كان المواطن الرقمي قد أرسل مواد سرية عبر الحدود. وعلى وجه الخصوص، أثبتت مواقع

التواصل المهني مثل لينكد إن أنها مكان مناسب تمامًا لتوظيف الوكلاء الصينيين.

منذ دخولها المجال الرقمي لوسائل التواصل الاجتماعي، أصبحت الصين خصمًا عدوانيًا للغاية في مجال الاستخبارات الإلكترونية. وقد حققت الصين ذلك من خلال استغلال أكثر العلاقات الاجتماعية عبر الإنترنت براءةً في البداية لزيادة مخزونها من المعلومات الاستخباراتية الخارجية. ثانيًا، فرضت الصين في الوقت نفسه نظامًا اجتماعيًا داخليًا صارمًا.

اللوائح الإعلامية القائمة على مفهوم "سيادة الإنترنت" والتي تضر بالدول الديمقراطية الغربية وبمواطني الصين أنفسهم. ووسائل التواصل الاجتماعي توفر وسيلة أكثر سلاسة وسرية وفعالية لتجنيد العملاء الصينيين.

باستخدام أسلوب دراسة الحالة، سيقدم هذا الفصل حالة توظيف وكلاء صينيين قبل ظهور وسائل التواصل الاجتماعي وحالة توظيف وكلاء صينيين بعد ظهور وسائل التواصل الاجتماعي، حيث تم إجراء الحالة الأخيرة من خلال موقع التواصل المهني LinkedIn.

وتجنيد العملاء الصينيين عبر وسائل التواصل الاجتماعي يجب أن يكون مصدر قلق خاص لمجتمع

الاستخبارات الأمريكي بسبب الطرق التي تُسرِّع بها وتخفي المراحل المبكرة من تجنيد العملاء.

دورة تجنيد الاستخبارات البشرية:

غالبًا يُطلَق على الاستخبارات البشرية أو HUMINT اسم "ثاني أقدم مهنة في العالم". ورغم اختلاف الآراء حول ما يشكل "الذكاء" تحديدًا، إلا أن هناك إجماعًا واسعًا فيما يتعلق بخطوات عملية تجنيد العملاء البشريين. يُعرف هذا أيضًا باسم "دورة استقطاب العملاء" التي تستخدمها وكالات الاستخبارات المختلفة.

تتضمن الخطوات الخمس لهذه الدورة ما يلي:

- الاستهداف أو الرصد،
- التقييم.
- التجنيد.
- التعامل.
- الإنهاء.

الاستهداف: هو التحديد الأولي للأفراد الذين يُعتقد أن لديهم إمكانية الوصول إلى المعلومات الاستخباراتية. والتقييم هو عملية البحث واتخاذ القرار التي تسعى إلى تضييق نطاق الموارد البشرية المحتملة. ويُعد التجنيد

خطوة حاسمة يقوم فيها ضابط المخابرات "بعرض" الأصول البشرية المحتملة، وتبدأ العلاقة السرية الرسمية.

والتعامل هو العلاقة المستمرة بين العميل المجند والجهة المسؤولة عنه، حيث يتم تزويد الجهة المسؤولة بالمعلومات الاستخباراتية، غالبًا في مقابل المال أو البضائع أو غيرها من المنافع. وإنهاء العلاقة هو حلّ العلاقة السرية. وهناك عدة أسباب، سواء كان ذلك تعريض الأصول البشرية للخطر، أو نقص إنتاجية الأصول، أو تغيير في متطلبات الاستخبارات الخاصة بالوكالة.

مع تقدم ضباط المخابرات في حياتهم المهنية وانتقالهم حول العالم، قد يقومون أيضًا "بتسليم" الأصول إلى زملائهم ضباط المخابرات من أجل مواصلة تدفق المعلومات الاستخباراتية، إذا لم يكن إنهاء الخدمة ضروريًا.

توظيف وكلاء اللغة الصينية التقليدية

كما يشهد العديد من علماء الصينيات والمؤرخين، فإن للصين تاريخًا طويلًا مرتبطًا بثاني أقدم مهنة في العالم، والتي يعود تاريخها إلى القرن الخامس قبل الميلاد على الأقل. وفي كتاب: "فن الحرب" لسن تزو، يتناول الفصل الأخير من كتاب الاستراتيجي العسكري الشهير موضوع

التجسس بشكل حصري. بحسب سن تزو، فإن الجواسيس يأتون في 5 أنواع مختلفة ويمكن استخدامهم في: العمليات وجمع المعلومات وعمليات الخداع والعديد من المهام الأخرى من أجل خدمة الدولة أو تأمين النجاحات العسكرية.

على مر القرون، ومع تغير أهداف الصين العسكرية وسياستها الخارجية، تغير جهاز استخباراتها وتكتيكاته أيضًا. قبل إقامة العلاقات الدبلوماسية مع الولايات المتحدة في عام 1979، كانت فرص التجسس الصيني قليلة ونادرة، وكانت تُنفذ بشكل شبه حصري من قبل مواطنين صينيين كُلفوا من قبل حكومتهم ثم أُرسلوا إلى الخارج.

في الواقع، قبل عام 2009، كانت قضية التجسس الصينية الوحيدة التي وصلت إلى المحاكمة هي قضية لاري وو تاي تشين، الذي كان مترجمًا لوكالة المخابرات المركزية في خدمة معلومات البث الأجنبي.

جُند تشين في أربعينات القرن الماضي، وتقاضى مئات الآلاف من الدولارات على مدى 4 عقود، وتم التعامل معه وفقًا لمعايير العمل الاستخباراتي الغربي. جُنِّد تشين أثناء عمله في مكتب الاتصال التابع للجيش الأمريكي في فوتشو، واستمر في التجسس بعد تاريخ تقاعده من الجيش. على مدار حياته، زود تشين المخابرات الصينية

بنصوص استجواب السجناء الصينيين خلال الحرب الكورية، وهويات موظفي وكالة المخابرات المركزية، بالإضافة إلى عشرات الوثائق السرية لوكالة المخابرات المركزية ومكتب التحقيقات الفيدرالي.

كان مسؤولو وزارة الأمن العام التابعون لتشين يلتقون به عادةً في هونغ كونغ أو البر الرئيس، لكنهم كانوا يزودونه أيضًا بساعٍ يقابله في مركز تجاري في تورنتو لاستعادة أي وثائق ذات صلة بحوزته.

المشرفون.

أشار تشين إلى استعداده للقاء القائمين على رعايته من خلال إرسال رسائل إلى عناوين في هونغ كونغ أو غوانزو. وأفادت مصادر أن الصينيين كان لديهم خطة طارئة لتهريب تشين من الولايات المتحدة باستخدام ضابط مخابرات متنكر في زي كاهن يعيش في نيويورك. بفضل أراضيها الشاسعة وإيمانها الراسخ بسيادة الدولة، نادرًا ما أرسلت الصين ضباطها إلى الخارج لإجراء عمليات تجنيد في مواقعهم.

الاستثناء من ذلك سيكون عندما أرسل الحزب الشيوعي الصيني ضباطًا إلى الخارج خلال السنوات التي سبقت عام 1949، عندما تأسست جمهورية الصين الشعبية. بعد عام 1949، وبعد قطع علاقاتها مع الاتحاد

السوفيتي، دخلت المخابرات الصينية مرحلة انعزالية استمرت حتى يومنا هذا.

بينما اجتازت الصين عدة عقود من العمل الدبلوماسي المحدود، كيَّفَت المخابرات الصينية منهجيتها العرقية في تجنيد البشر وفقًا لذلك. بدأت المخابرات الصينية، التي تعمل في ظل أنواع مختلفة من القيود الانعزالية، في تكييف تكتيكاتها العملياتية من أجل تقليل حجم الاتصال بين الضباط والعملاء.

منذ منتصف القرن 20 حتى أواخره، أضافت المخابرات الصينية أيضًا أسلوبًا آخر إلى ترسانة أدواتها في مجال الاستخبارات البشرية:

تجنيد العملاء و"زرعهم" من خلال إقناعهم بالتقدم لشغل مناصب حساسة داخل حكومة الولايات المتحدة. وكان المثال الكلاسيكي على ذلك هو حالة المواطن الأمريكي المجنس تشي ماك. بعد هجرته إلى هونغ كونغ، بدأ تشي بتزويد الصينيين بمخططات السفن الحربية الأمريكية وقوائم الزوار لقادة البحرية الأمريكية الذين يزورون المدينة الساحلية.

في سبعينيات القرن 20، هاجر تشي إلى الولايات المتحدة، حيث حصل على جنسيته في عام 1985. وفي عام 1996، حصل تشي على تصريح أمني من خلال عمله في شركة باور باراغون. وعلى مدى أكثر من 40 عامًا، قدم

تشي معلومات استخباراتية للصينيين وساعد في إدارة أصول أخرى مقرها الولايات المتحدة.

قبل اعتقاله في عام 2005، قدم تشي معلومات استخباراتية حول محرك القيادة الإلكتروني الهادئ، الذي كان يزود غواصات البحرية الأمريكية الجديدة من فئة فيرجينيا بالطاقة وتقنيات حساسة مماثلة. بحسب الخبير الصيني بيتر ماتيس، فإن جهاز الاستخبارات الصيني اليوم يتألف من عدة مؤسسات، ضمنها:

- وزارة أمن الدولة.
- وزارة الأمن العام.
- الإدارة الثانية لهيئة الأركان العامة لجيش التحرير الشعبي.
- مكتب الاتصال التابع للإدارة السياسية العامة.

ولا تزال وزارة أمن الدولة الصينية تجمع كميات هائلة من المعلومات الاستخباراتية البشرية عن طريق استغلال كبار المسؤولين. ومن أجل رصد وتقييم الأفراد الذين قد يكونون منفتحين على التوظيف، اعتمد الصينيون تقليديًا على المواد مفتوحة المصدر التي جُمِعَت من الشركات الأمريكية والجمعيات التقنية والجامعات. ورغم أنها غير مصنفة، إلا أنه لا ينبغي الاستهانة بقيمة المعلومات الاستخباراتية مفتوحة المصدر، وبخاصة عندما يجمعها ويحللها خصم حقيقي.

بالمقارنة مع عمليات التجنيد عالية المخاطر التي تقوم بها وكالات الاستخبارات الغربية خارج حدودها، يفضل الصينيون ممارسة درجة عالية من السيطرة على بيئة التجنيد، كما يتضح من تفضيلهم لتجنيد الأصول البشرية داخل جمهورية الصين الشعبية. هذا التفضيل، الذي أشار إليه الباحث في مجال الاستخبارات الصينية نيكولاس إفتيمياديس، يمكن تلخيصه فيما يلي:

يفضل جهاز أمن الدولة الصيني تجنيد عملاء في الصين. وتجنيد الرعايا الأجانب على أرض المرء يعتبر عادةً طريقة آمنة وفعالة من حيث التكلفة للقيام بالتجسس. وتتمثل الفوائد الرئيسة في توفير بيئة آمنة لموظف القضية وعدم وجود عواقب في حال رفض العميل المحتمل عرض التوظيف. وتتمثل إحدى الفوائد الثانوية لتجنيد عملاء التجسس في بلد المرء في أن الحكومات لا تحتاج إلى تحمل تكلفة إبقاء ضباط العمليات وعائلاتهم في الخارج. بالإضافة إلى ذلك، تعتبر هذه الطريقة آمنة بشكل عام فيما يتعلق بمخاوف مكافحة التجسس الأجنبية.

من أجل استدراج الرعايا الأجانب إلى الأراضي الصينية، تشمل أشكال التغطية الشائعة توجيه دعوات لخبراء الصناعة والمسؤولين الحكوميين والأكاديميين لزيارة الصين في جولة محاضرات أو مقابلة عمل مطولة

تستغرق عدة أيام. وقد تتضمن "مقابلات العمل" السرية هذه اجتماعات مهنية، ومجموعة كبيرة من المناسبات الاجتماعية، وغالبًا ما تتضمن كمية كبيرة من الكحول.

في مرحلة معينة خلال هذه العملية المعقدة المصممة بعناية، يُعرض على المدعو فرصة مواصلة علاقته مع الكيان الخفي (غالبًا تكون جامعة صينية أو مؤسسة بحثية تابعة لوزارة الأمن الداخلي أو شركة ترعاها الدولة) وتزويدهم بمواد أكثر مما اتُفِق عليه. وفي أحيانٍ كثيرةٍ، يكون هذا الطلب متعلقًا بمواد سرية.

إذا تحولت العلاقة شبه المهنية إلى منطقة سرية وتم التجنيد فعليًا، فسوف يوقع العميل اتفاقية، يُمنَح بموجبها مبلغًا من المال ويعد مشغليه الصينيين باستمرار "التعاون" في وقت لاحق.

وبمجرد تجنيد العملاء أو المتعاونين في الصين، يجري إرسالهم مرة أخرى إلى الولايات المتحدة بمهام لجمع معلومات استخباراتية حول العلوم أو التكنولوجيا أو المواد السرية التي تهم جمهورية الصين الشعبية. وعلى غرار بيئة التوظيف الخاضعة للرقابة، غالبًا يقتصر التعامل مع المصادر داخل المخابرات الصينية على الاجتماعات وجهًا لوجه على الأراضي الصينية، وعادةً يكون ذلك عندما يدعي العميل البشري أنه يزور الصين لأغراض العمل أو للترفيه.

يمكن الحفاظ على هذا النوع من التغطية لعقود دون أن يلفت انتباه أجهزة مكافحة التجسس الأمريكية، حيث إن الصين غالبًا يكون لديها اهتمام خاص بالأهداف العلمية والتكنولوجية الحساسة.

وفي حين أن العديد من وكالات الاستخبارات الأكثر نشاطًا في العالم تعتمد على تدفق مستمر للأموال لتحفيز عملائها، فإن الكادر الصيني المتجانس عرقيًا من الأصول البشرية غالبًا يكون مدفوعًا في البداية بشعور بالالتزام الثقافي والاجتماعي.

بالنسبة لغير الصينيين الذين يجري تجنيدهم، فغالبًا يكونون متحدثين بطلاقة للغة الماندرين ولديهم فهم ممتاز للغة وفهم عميق وحب للثقافة. وهذه الطبقات المتعددة الأوجه من الدوافع تزيد ضبابية خطوط العلاقة بين الفئات الاجتماعية والمهنية والسرية.

التوظيف السري في وسائل التواصل الاجتماعي:

تأسس LinkedIn كموقع للتواصل المهني في عام 2003، واعتبارًا من عام 2019، ضم أكثر من 660 مليون مستخدم في 200 دولة حول العالم. وفي ظلّ الإنترنت المتزايد الانقسام والتسييس، يبرز موقع LinkedIn بفضل

جاذبيته متعددة الثقافات. وعلى النقيض من الاستبعاد الصارم للعديد من مواقع التواصل الاجتماعي الغربية مثل فيسبوك وتويتر، سُمح لـ LinkedIn بالعمل في العديد من الدول ذات السيادة الرقمية مثل الصين وإيران وحتى كوريا الشمالية.

رغم أن هذا قد يبدو مفيدًا من وجهة نظر اقتصادية عالمية، إلا أن العديد من الاستخدامات الحديثة لـ LinkedIn من قبل قوى إلكترونية معادية تحكي قصة تحذيرية. رغم عدم الإبلاغ عن المدى الكامل لتورط وكالات الاستخبارات الأجنبية على الموقع، إلا أن هناك العديد من المنافذ الصحفية التي نشرت تقارير عن العديد من الحوادث في السنوات الأخيرة.

في 24 يوليو 2015، أرسلت وكالة الاستخبارات الداخلية البريطانية MI-5، بريدًا إلكترونيًا كان بمنزلة "تنبيه تجسس من جهاز الأمن". ومن بين النتائج والتحذيرات الرئيسة الواردة في البريد الإلكتروني، كانت هناك ملاحظة مفادها أن

"أجهزة الاستخبارات الأجنبية المعادية تستخدم بشكل متزايد موقع LinkedIn للعثور على موظفي حكومة صاحبة الجلالة الحاليين والسابقين والتواصل معهم وبدء استقطابهم وتوظيفهم".

في ديسمبر 2017، أفادت وكالة الاستخبارات الداخلية الألمانية أن المخابرات الصينية أنشأت شبكة من الملفات الشخصية المزيفة على LinkedIn التي اتصلت بأكثر من 10000 مواطن ألماني. وشارك مكتب حماية الدستور بعض هذه الملفات الشخصية علنًا مع وكالة رويترز الإخبارية، وأفادت بعد مراجعتها أن بعض هذه الملفات الشخصية تضم "دبلوماسيين وسياسيين كبار من عدة دول أوروبية" ضمن علاقاتها.

في أكتوبر 2018، تلقت صحيفة لوفيجارو الفرنسية تقريرًا مشتركًا مسربًا من المديرية العامة للأمن الداخلي والمديرية العامة للأمن الخارجي الفرنسيتين (وكذلك وكالات الاستخبارات الداخلية والخارجية الفرنسية).

وأفادت الوثيقة بأن موظفي الدولة الفرنسية كانوا مذنبين بـ "السذاجة" فيما يتعلق بوكلاء المخابرات الصينية الذين سعوا للوصول إليهم من خلال موقع LinkedIn. ويُزعم أن آلاف الموظفين الحكوميين الفرنسيين قد تواصل معهم أشخاص يحملون صورًا رمزية صينية، ما دفع المخابرات الفرنسية إلى تغيير إجراءاتها الأمنية في يونيو 2017 والرد على الهجمات "ضربة بضربة" من تلك النقطة فصاعدًا.

في أغسطس 2018، أعلن مسؤول استخباراتي أمريكي علنًا أن الصين تشن حملة "عدوانية للغاية" لاستهداف مستخدمي LinkedIn الذين لديهم إمكانية الوصول إلى مواد سرية.

قال مسؤولون في الاستخبارات الأمريكية إن روسيا وإيران وكوريا الشمالية ودول أخرى تستخدم أيضًا موقع LinkedIn ومنصات مماثلة لتجنيد العملاء، لكن "الصين هي الأكثر إنتاجية وتشكل أكبر تهديد."

المنهجية

بالنظر إلى المراحل المختلفة لتجنيد الوكلاء، وخصوصية النهج الصيني، وتعقيدات وسائل التواصل الاجتماعي، فإن أسلوب دراسة الحالة هو الأمثل لدراسة هذا الموضوع وإدخاله في نقاش البحث الأوسع.

أول حالة سيتم دراستها هي حالة بيتر لي، وهو مواطن أمريكي متجنس من تايوان، والذي أدت رحلاته التجارية المتكررة إلى البر الرئيسي للصين إلى عملية تجنيد نموذجية للعملاء الصينيين. ودراسة الحالة الثانية هي حالة كيفن مالوري، وهو ضابط سابق في وكالة المخابرات المركزية، دفعته ظروف حياته إلى لصق سيرته الذاتية على موقع LinkedIn والرد على "مُوظِّف توظيف" صيني أقنع

مالوري في النهاية بأن مصلحته تقتضي تسليم وثائق سرية إلى المخابرات الصينية مقابل المال.

فيما يتعلق بمعايير اختيار الحالات، كانت السمات التالية من أسباب اختيار الحالات: ثراء البيانات، ونموذجية ظروف خلفية الحالة، والأهمية الجوهرية.

أولًا، اختيرت هذه الحالات نظرًا لتغطيتها العالية نسبيًا في التقارير الصحفية والحكومية الرسمية. ورغم أن حالات أخرى للتجسس الصيني وتجنيد العملاء الأمريكيين حظيت بتغطية في وسائل الإعلام العامة، إلا أن العديد من هذه الحالات الأخرى لا تحتوي على وثائق مصدرية أولية أو المستوى نفسه من التفاصيل والموثوقية.

ثانيًا، اختيرت الحالات لتمثيلها النموذجي لنهج الصين في تجنيد العملاء داخل وسائل التواصل الاجتماعي وخارجها.

دراسة حالة رقم 1: بيتر لي: مفكر، مترجم، عالم، جاسوس

ظاهريًا، من غير المرجح أن يتم اختيار بيتر هونغ-يي لي ليكون البطل الرئيس في فيلم إثارة تجسسي هوليوودي. بصفته عالمًا هادئًا ومتواضعًا، لم يكن لدى لي

أي منصب عسكري أو لم يتلق تدريبًا في مجال التجسس، ولكنه كان باحثًا ماهرًا للغاية برع في مجال الاندماج بالقصور الذاتي (ICF) للأسلحة النووية. كان والد لي جنرالًا في الجيش القومي الصيني الذي طرده ماو تسي تونغ في نهاية المطاف.

بعد أن نشأ لي في تايوان، التحق بجامعة تايوان الوطنية ثم انتقل لاحقًا إلى الولايات المتحدة، حيث حصل على الجنسية الأمريكية في عام 1975. بعد التخرج، حصل لي على عقد بحثي في مجال الاحتراق الداخلي مع مختبر لورانس ليفرمور الوطني (ليفرمور) من خلال شركة TRW في كاليفورنيا. سرعان ما أكسبته موهبة لي في مجال الأبحاث النووية منصب رئيس فريق أبحاث الليزر في ليفرمور.

في عام 1980، عاد لي إلى الصين، حيث عمل كمترجم لفريق من علماء مختبر ليفرمور. وخلال إقامته هناك، زار عالم صيني غرفة لي في الفندق ذات ليلة. رغم أنه لم يشارك الكثير من التفاصيل، إلا أن لي ذكر الاجتماع لأحد زملائه في العمل. قام زميل العمل، الذي كان على دراية بسياسة الأمن الخاصة بالشركة، بالإبلاغ على الفور عن الاجتماع المفاجئ إلى أمن ليفرمور عند عودتهم إلى الولايات المتحدة. وبسبب فشل لي في الإبلاغ عن الحادث للأمن وأنه بدأ تبادلًا اجتماعيًا علنيًا واستخباراتيًا سريًا مع

الصين استمر لعقود من الزمن، ما أدى إلى تحقيق من قبل مكتب التحقيقات الفيدرالي ومقاضاة في نهاية المطاف.

إلى جانب زوجته هذه المرة، عاد لي بسرعة إلى الصين بعد هذه الزيارة الأولى، وقضى خمسة أسابيع في ديسمبر 1981 ويناير 1982 يعمل في معهد شنغهاي للبصريات والليزر. بعد أن رأى لي الظروف المزرية للمختبر الصيني مقارنة بما كان لدى الولايات المتحدة، سعى إلى تحسين الظروف في الصين. في إحدى رحلاته المبكرة إلى الصين، التقى لي بتشن نينغ كوان، الباحث في مجال المتفجرات الذي كان بمنزلة مضيف لأهداف استخباراتية أمريكية بالغة الأهمية للصين، وشملت في مرحلة ما مدير مختبر لوس ألاموس، هارولد أغنيو.

بعد لقاء تشن، بدأ لي علاقة استمرت 16 عامًا مع المخابرات الصينية، تم توثيقها من خلال مراسلات مع علماء صينيين تضمنت أكثر من ستمائة مكالمة هاتفية ورسالة، ورسائل البريد الإلكتروني. وفي عام 1984، بدأ لي العمل في مختبر لوس ألاموس، بالتزامن مع استمراره في زياراته المنتظمة إلى البر الرئيس الصيني. في عام 1985، خلال رحلة منفردة إلى مركز أبحاث الأسلحة النووية في ميانيانغ، زاره تشن في غرفته بالفندق مرة أخرى. بهدوء ومهارة، بدأ تشين بطرح سلسلة من الأسئلة على لي وتعمقت في المعلومات السرية.

كان لي مترددًا في البداية، لكن بعد أن أكد تشين على الوضع المؤسف، بعد أن علم لي بظروف منشآت الأبحاث النووية الصينية وكيف يمكنه ببساطة أن يومئ برأسه "نعم" أو "لا" على أسئلته، استسلم وبدأ يجيب أولًا بالإيماءات ثم بجمل كاملة. في اليوم التالي، نُقِل لي إلى غرفة فندق أخرى، هذه المرة كانت مليئة بعلماء أسلحة صينيين طرحوا أسئلة حساسة مماثلة لساعات، والتي أجاب عليها لي على الفور.

إذا كانت العلاقة قد تذبذبت بين المهنية والسرية من قبل، ففي غرفة الفندق الثانية، المحاطة بحشد كبير من الشهود، لم يكن هناك شك في أن الصين حولت لي فعليًا من مجرد معارف متحمسين إلى جاسوس كامل.

في عام 1985، فتح مكتب التحقيقات الفيدرالي تحقيقًا في التجسس وحصل على موافقة للمراقبة الإلكترونية للي. ولسنوات، لم يظهر أي شيء جوهري، لكن في عام 1997، بعد عودتها إلى المنزل من الصين، اكتشفت زوجة لي ميكروفونًا تابعًا لمكتب التحقيقات الفيدرالي في فتحة تهوية بالسقف أثناء قيامها بالتنظيف. أصبح مكتب التحقيقات الفيدرالي الآن على علم بأن تسجيلاتهم السرية قد تم اختراقها، لذلك طلبوا مقابلة لي في فندق في سانتا باربرا. وفي النهاية، اعترف لي بمشاركة معلومات الدفاع الوطني مع الصين لأكثر من عقد من

الزمان. وذكر لي أيضًا أن دوافعه تنبع إلى حد كبير من رغبته في إرضاء والده، ومن انعدام الأمن الشخصي، ومن ما وصفه محامي لي بـ "الحماس العلمي".

رغم أن التحقيقات الحكومية شككت لاحقًا في ملاحقة مكتب التحقيقات الفيدرالي ووزارة العدل لبيتر لي، إلا أن عملية توظيفه كعميل تُعد بمنزلة مثال نموذجي لأسلوب عمل الاستخبارات البشرية الصينية.

دراسة حالة رقم 2: كيفن مالوري: موظف سابق في قسم الحالات يبحث عن وظيفة حالية

تُعد عملية تجنيد كيفن مالوري الناجحة مثالًا على أساليب تجنيد العملاء المتطورة في الصين. في عام 2017، تم اكتشاف أن مالوري، وهو ضابط سابق في وكالة المخابرات المركزية ومتحدث بطلاقة باللغة الصينية، قد جرى رصده وتقييمه وتجنيده في نهاية المطاف من قبل المخابرات الصينية عبر موقع LinkedIn.

قبل تجنيده، شغل مالوري مناصب ضباط في وكالة المخابرات المركزية (CIA) ووكالة استخبارات الدفاع (DIA)، وكلاهما منحه تصاريح أمنية سرية للغاية. ترك مالوري وظيفته الحكومية في عام 2012، وبحلول عام 2017، كان متأخرًا في سداد أقساط رهن عقاري، ما جعله هدفًا للتجنيد. بدأ اتصال الصين مع مالوري عبر LinkedIn

في فبراير 2017 من قبل شخص قال مالوري إنه بدا وكأنه صائد رؤوس (تبين لاحقًا أنه شخص يدعى مايكل يانغ) يعرض عليه وظيفة كمستشار لمركز أبحاث صيني. أدرجت إفادة خطية صادرة عن مكتب التحقيقات الفيدرالي اسم مركز الأبحاث: "أكاديمية شنغهاي للعلوم الاجتماعية." كما تضمنت الإفادة نفسها تقييم مكتب التحقيقات الفيدرالي بأن "مكتب أمن الدولة في شنغهاي، وهو مكون فرعي من وزارة أمن الدولة، لديه علاقة وثيقة مع الأكاديمية المذكورة.

وقد خلص مكتب التحقيقات الفيدرالي كذلك إلى أن ضباط المخابرات في وحدة مكافحة الإرهاب قد استخدموا أيضًا انتماءهم إلى وحدة مكافحة الإرهاب كغطاء لهوياتهم. وبعد عدة رسائل على LinkedIn، قام يانغ، الذي لا يزال يتظاهر بأنه باحث عن الكفاءات، بترتيب مكالمة هاتفية مع مالوري وموظف في مركز الأبحاث.

قام مالوري برحلتين إلى الصين في عام 2017، وفي إحدى المرات وافق على مقابلة 3 رجال في غرفة فندق. وبمجرد دخوله جناح الفندق في شنغهاي، استُجوِب مالوري بشأن السياسة الخارجية لإدارة ترامب، وكذلك للحصول على تفاصيل حول نظام صواريخ ثاد، وسُئل عن موقف الولايات المتحدة تجاه بحر الصين الجنوبي.

في الرحلة الثانية، حصل مالوري على هاتف سامسونج جالاكسي مُجهز خصيصًا بتطبيق دردشة مشفر استخدمه للتواصل مع يانغ. تمكن مكتب التحقيقات الفيدرالي من استعادة هذه المحادثات والكشف عن تفاصيل العلاقة بين مالوري ويانغ. بدا أن يانغ يضغط على مالوري للحصول على مزيد من المعلومات التي قد تكون مفيدة، مع التركيز على سلامة مالوري.

من ناحية أخرى، بدا أن مالوري يضغط على يانغ للحصول على تعويض مالي أعلى، نظرًا للمخاطر التي كان يتعرض لها من خلال تقديم هذه الوثائق. وكشف تحليل الطب الشرعي الإضافي الذي أجراه مكتب التحقيقات الفيدرالي للهاتف ومحتوياته أن مالوري أكمل جميع الخطوات المطلوبة لنقل ما لا يقل عن 5 وثائق حكومية سرية، إحداها تحتوي على معلومات تعريفية شخصية لمصادر بشرية تابعة للحكومة الأمريكية.

وأُرسِلَت وثيقتان على الأقل، ولاحقًا التُقِطَت الاتصالات بين مالوري ويانغ بشأن هاتين الوثيقتين من الجهاز. وقد افترض مالوري أن جهات اتصاله الصينية كانت ضباط مخابرات، لكنه مع ذلك، استمر في تزويده بما تم تحديده من خلال تحقيق أجراه مكتب التحقيقات الفيدرالي على أنه وثائق سرية.

خلال محاكمته، كُشِف عن أن مالوري أرسل إلى يانغ وثيقتين على الأقل، إحداها توضح عملية سرية مقترحة لوكالة الاستخبارات الدفاعية. ورغم أن العديد من تفاصيل العملية المقترحة نُقِيحَت، إلا أن شهادة المحكمة أشارت إلى أن العملية كانت ستتضمن استخدام مالوري غطاءً غير رسمي في شركة لها وجود في الصين، لكن مالكيها (الذين أطلق عليهم في المحكمة اسم "جونسون") كانوا يتعاونون بالفعل مع حكومة الولايات المتحدة. كان هدف مالوري جمع معلومات استخباراتية حول العلوم والتكنولوجيا.

وأدلى الشاهد روبرت أمبروز، الذي أشرف على العمليات السرية في وكالة استخبارات الدفاع، بشهادته أمام المحكمة قائلًا إن نسخة معدلة من هذه الخطة قد نُفِّذت بالفعل. ومع ذلك، في عام 2011، فُصِل مالوري من وكالة الاستخبارات الدفاعية بعد أن شارك تفاصيل العملية المقترحة مع متعاقد استخباراتي خاص. قُبِض على مالوري عند عودته الثانية من شنغهاي عندما عثر موظفو الجمارك على 16500 دولار نقدًا غير مصرح بها بحوزته. وبحسب ما ورد، حصل مالوري على مبلغ إجمالي قدره 25 ألف دولار مقابل تقديم وثائق سرية.

وفي محاكمته بتهمة التجسس عام 2018، اطلع المحلفون على هذه الوثائق، بالإضافة إلى وثائق سرية

أخرى تتعلق بعمليات الاستخبارات الدفاعية وتحليلات وكالة المخابرات المركزية بشأن القدرات الاستخباراتية لدولة أخرى والتي قام مالوري بتحميلها على بطاقات الذاكرة.

وقد تضمنت أدلة المحاكمة لقطات فيديو لمالوري وهو يقوم بمسح وثائق سرية للغاية وسرية في متجر فيديكس ثم يقوم بتحميل الوثائق على بطاقات ذاكرة، كما أوضحت سجلات المحكمة بالتفصيل الوضع المالي غير المستقر لمالوري، موضحة كيف كان عليه متأخرًا في سداد أقساط الرهن العقاري بقيمة 12205.32 دولارًا، وديون بطاقات ائتمان بقيمة 30000 دولارًا، وديون أخرى.

في يونيو 2018، أدين مالوري بالتآمر لتسليم معلومات الدفاع الوطني، ومحاولة تسليمها، وتسليمها فعليًا لمساعدة حكومة أجنبية، والإدلاء بتصريحات كاذبة جوهريًا. وفي مايو 2019، حُكم على مالوري بالسجن 20 عامًا تليها 5 سنوات من الإفراج المشروط.

تحليل دراسة الحالة

كما يتضح من الحالتين، فإن مراحل رصد وتقييم تجنيد العملاء في الصين غالبًا تبدأ كمواجهات بريئة، خالية مما قد تعتبره العديد من وكالات الاستخبارات الأجنبية

أساليب عمل متطورة. ولا توجد عمليات تسليم سرية، ولا مراقبة عالية السرعة، ولا حفلات كوكتيل؛ ببساطة يتواصل أحد المحترفين مع آخر، مع توقع ضمني لعلاقة أعمق. وهناك العديد من الجوانب الرئيسة لتكنولوجيا وسائل التواصل الاجتماعي التي غيرت هذه العملية بشكل كبير وتستحق الاستكشاف بشكل أعمق.

حتى يومنا هذا، تستقبل الصين العديد من الصينيين من أصول عرقية مثل لي كزوار، والذين قد يكونون أهدافًا استخباراتية محتملة، ولكن على عكس الحرب الباردة، فإن التكنولوجيا الحالية تمكن دولًا مثل الصين من القيام بالكثير من عمليات الرصد مسبقًا.

قبل ظهور وسائل التواصل الاجتماعي، كان تحديد هدف معين على الساحة المهنية العالمية مهمة أكثر صعوبة بكثير. كما يتضح من قضية مالوري، فإن مرحلة تحديد العملاء وتجنيدهم أصبحت أسهل بكثير مع ظهور وسائل التواصل الاجتماعي والملفات الشخصية الغنية بالتفاصيل التي تصاحبها.

على موقع LinkedIn، يتم تذكير المستخدمين بنسبة اكتمال ملفاتهم الشخصية. يُقدّم موقع LinkedIn تقييمًا إيجابيًا للمستخدمين الذين يختارون مشاركة معلومات شخصية متنوعة، وتقييمًا سلبيًا (على شكل نوافذ منبثقة

ورسائل تذكير عبر البريد الإلكتروني) للمستخدمين الذين يرفضون مشاركة هذه التفاصيل.

ويُولي LinkedIn اهتمامًا خاصًا للمستخدمين الذين يختارون عدم إضافة صورة شخصية، ويسألهم بشكل دوري عن سبب ذلك. بالنسبة لضابط المخابرات الصيني الحديث، توفر ثقافة LinkedIn الرقمية التي تشجع على الانفتاح مجموعة بيانات يسهل الوصول إليها للغاية لأهداف استخباراتية محتملة.

التقييم في وسائل التواصل الاجتماعي

على غرار الرصد من خلال وسائل التواصل الاجتماعي، فإن تقييم الأهداف أسهل بكثير في وسائل التواصل الاجتماعي، حيث تسمح مواقع مثل LinkedIn للمستخدمين بالبحث عن الملفات الشخصية بناءً على مجموعة واسعة من الخصائص، ما يتيح للمسؤولين المحتملين فرز وتصفية الملفات الشخصية بناءً على مجموعات المهارات المطلوبة والخبرة المهنية.

بالإضافة إلى ذلك، يسمح موقع LinkedIn للمستخدمين بتصدير ملفاتهم الشخصية بتنسيقات ملفات متنوعة، ما يعزز سهولة نقل المعلومات وفرزها، بفضل وسائل التواصل الاجتماعي. في حين أن العملاء الصينيين ربما قاموا بتقييم لي على مدار عدة زيارات

منظمة بعناية إلى البر الرئيس الصيني، فإن تقييم هدف معاصر مثل مالوري يتطلب موارد أقل بكثير.

التوظيف عبر وسائل التواصل الاجتماعي

رغم أنه ليس موقع التواصل المهني الوحيد، إلا أن LinkedIn يتميز عن غيره من حيث الحصة السوقية.

لأن موقع LinkedIn مصمم خصيصًا لوكالات التوظيف الشرعية، فإنه لا يتطلب سوى القليل من الجهد من أي فرد للعثور على شخص يمتلك مجموعة محددة للغاية من المهارات والخبرات. وضمن الحدود الرقمية لـ LinkedIn، توجد أيضًا درجة عالية من الخصوصية، ما يجعلها مثالية للموظفين الذين يرغبون في البحث سرًا عن فرص عمل إضافية، أو الانشقاق إلى دولة أجنبية.

وعلى النقيض من أسلوب غرفة الفندق العلني الذي استخدمته المخابرات الصينية ضد بيتر لي، كان أسلوب مالوري أكثر خصوصية، وأكثر براءة، وأكثر روتينية من شخص يدعي أن لديه فرص عمل يدخل غرفة نوم مالوري.

إن العلاقة الحميمة والمسافة المتناقضة التي توفرها وسائل التواصل الاجتماعي تجعل الاتصال من الغرباء يبدو طبيعيًا، وبالتالي، أكثر براءة من الطرق الجسدية التي كانت سائدة خلال الحرب الباردة.

بالإضافة إلى ذلك، فإنّ هالة الشرعية التي يمنحها موقع LinkedIn تُضفي طابعًا فريدًا. على النقيض من جحافل الروبوتات المجهولة الهوية التي أنشأتها وكالة أبحاث الإنترنت الروسية، فإن جحافل مجندي الاستخبارات البشرية الصينيين هم من لحم ودم. وتهديد تجنيد العملاء الصينيين المعاصرين مزيج معقد من تقنيات الاستخبارات البشرية التقليدية والإمكانيات الحديثة للمجال الرقمي، فإنه يمثل تحديًا مستمرًا لوكالات الاستخبارات الغربية.

خاتمة

من خلال هذا الفحص لتجنيد العملاء الصينيين في وسائل التواصل الاجتماعي، يتضح أن عمليات الصين الإلكترونية الحديثة لا تركز فقط على استكشاف البنية التحتية الحيوية لأمريكا وسرقة ملكيتها الفكرية. فيما يتعلق بالأدوات الإلكترونية، يبدو أن وسيلة التواصل الاجتماعي "الناعمة" نسبيًا تمثل وسيلة جديدة قيّمة لتجنيد أجهزة الاستخبارات، وعلى هذا النحو، لا ينبغي تجاهلها باعتبارها مصدر قلق خطير في مجال مكافحة التجسس.

مع تزايد عدد ضباط المخابرات الصينيين الذين يتغلغلون في شبكات التواصل الاجتماعي، من الأهمية

بمكان أن يكون الباحثون من القطاعين العام والخاص على دراية بالقوى الدافعة التاريخية وراء هذه الأحداث.

والمحاكمة والحكم الأخيرين على كيفن مالوري يوضحان قدرة أمريكا على التحقيق في قضايا التجسس. ومع ذلك، يمكن بذل المزيد من الجهود لمنع هذا النوع من التجنيد الصيني قبل أن يبدأ. وأحد الجوانب البارزة لهذه المشكلة، والتي تميز حلها عن حل التجسس في الحرب الباردة، هو أن الكثير من البيانات ذات الصلة التي يمكن أن تساعد محللي الاستخبارات والباحثين الأكاديميين وصناع السياسات، موجودة حاليًا لدى شركات خاصة. وبسبب هذه الحقيقة، ينبغي التعامل مع خطوط البحث المستقبلية من خلال التعاون بين الدولة والقطاع الخاص.

بفضل مدخلات من كل من خبراء الاستخبارات وأصحاب المصلحة في القطاع الخاص، يستطيع مطورو وسائل التواصل الاجتماعي بناء منصات قوية قادرة على اكتشاف أو منع التدخل الأجنبي. كما أظهر تقرير لجنة 11 سبتمبر، فإن الدفاع الناجح عن الأمة لا يتحقق من خلال العزل البيروقراطي، بل من خلال التعاون المتضافر بين المهنيين في القطاعين العام والخاص.

ينبغي أن تستمر الأبحاث المستقبلية في هذا المجال في رصد التطورات في أساليب التجنيد الصينية في وسائل

التواصل الاجتماعي، مع إيلاء اهتمام خاص للتكتيكات والتقنيات والإجراءات التي تحاكي تلك التي استخدمتها الصين لقرون. وإذا امتلك خبراء القطاعين الخاص والعام فهمًا أكثر شمولية لكيفية تطور التهديد الاستخباراتي الصيني تاريخيًا، فسيكون بإمكان محللي وسائل الإعلام رصد وتقييم التهديدات المستقبلية لتجنيد العملاء الصينيين بشكل أفضل لصالح صانعي السياسات والمحللين ومسؤولي الأمن الأمريكيين.

سيرة ذاتية .... ممدوح الشيخ

عضو اتحاد كتاب مصر.

أولًا: ترجمات في معاجم وموسوعات

**ترجمة في الطبعة الأولى من: معجم البابطين للشعراء العرب المعاصرين، (مؤسسة البابطين، الكويت).

**ترجمة في الطبعة الأولى من: معجم أدباء مصر، (الهيئة العامة لقصور الثقافة، مصر).

**ترجمة في الطبعة الأولى من: الموسوعة الكبرى للشعراء العرب المعاصرين: 1956، 2006، إعداد وتقديم: فاطمة بوهراكة، المغرب، 2009، برعاية الشيخة أسماء بنت صقر القاسمي.

**ترجمة في الطبعة الأولى من: معجم الأدباء: من العصر الجاهلي حتى سنة 2002، كامل سليمان الجبوري، دار الكتب العلمية، بيروت، الطبعة الأولى، 2002، 1424 هجرية.

ثانيًا، ترجمات من الإنجليزية إلى العربية

**فضاء المقدس لا يعرف الفراغ: تاريخ الإلحاد السوفيتي، فيكتوريا سمولكين، ترجمة وتقديم، الناشر: مركز تكوين للدراسات والأبحاث – السعودية، 2022.

**علم نفس وادي السليكون، كاتي كوك، 2020، (تحت الطبع).

**رأسمالية مصاصي الدماء، المجتمعات المنقسمة والمستقبلات البديلة، باول كينيدي، 2018، (تحت الطبع، مدارات للنشر، مصر).

ثالثًا، مؤلفات منشورة ورقيًا

أولًا: دراسات في الظاهرة الدينية

**المسلمون ومؤامرات الإبادة، مكتبة مدبولي الصغير، مصر، 1994.

**الإسلاميون والعلمانيون من الحوار إلى الحرب

الطبعة الأولى، دار البيارق، الأردن، 1999.

الطبعة الثانية، مؤسسة حمادة للدراسات الجامعية والنشر والتوزيع، الأردن.

**الجماعات الإسلامية المصرية المتشددة في آتون 11 سبتمبر: مفارقات النشأة ومجازفات التحول، مكتبة مدبولي، مصر، 2005.

**مراجعات الإسلاميين (الجزء الأول)، تأليف بالاشتراك، مركز المسبار للدراسات والبحوث، الإمارات، سلسلة كتاب المسبار الشهري، العدد السادس والثلاثون، ديسمبر 2009.

**السلفيون من الظل إلى قلب المشهد، دار أخبار اليوم، مصر، 2012.

**دراما محمد رمضان والإرهاب: الملائكة والشياطين والعدالة الناجزة، توزيع: مكتبات أخبار اليوم (مصر)، 2019.

ثانيًا: مؤلفات إبداعية منشورة

**نقوش على قبور الشهداء، ديوان شعر، مركز يافا للدراسات والأبحاث، مصر، 1996.
**الحلم المسروق (ديوان شعر بالعامية)، مركز يافا للدراسات والأبحاث، مصر، 2003.
**الندى والموت (ديوان شعر)، مركز يافا للدراسات والأبحاث، مصر، 2003 .
**عاصمة للبيع (مسرحية)، دائرة الثقافة والإعلام بإمارة الشارقة، دولة الإمارات، 2000.
**القاهرة.. بيروت.. باريس (رواية)، الدار العربية للعلوم، بيروت، 2006 .
**الممر إلى السماء، (رواية)، دار لوسيل للنشر، قطر، 2019.
**إن الغريب حزين حيثما كانا: سيرة لم يكتبها موسى ابن ميمون (رواية)، توزيع: مكتبات أخبار اليوم (مصر)، 2019.
**رائحة الضجر، (رواية)، دار البشير للثقافة والعلوم، مصر، 2023.
ثالثًا: مؤلفات أخرى منشورة
**أشهر الأحلام في التاريخ، مكتبة ابن سينا، مصر، 1993.
**التنبؤات والأحلام من الخرافة إلى العلم، دار التضامن، لبنان، 1996.
**ثقافة قبول الآخر، مكتبة الإيمان، مصر، مكتبة جزيرة الورد، مصر، 2007.

**مدخل إلى عالم الظواهر الخارقة، مكتبة بيروت، سلطنة عمان، شركة دلتا، مصر، 2007.
**التجسس التكنولوجي: سرقة الأسرار الاقتصادية والتقنية (دراسة في المجتمع ما بعد الصناعي)، مكتبة بيروت، سلطنة عمان، شركة دلتا، مصر، 2007.
**ثقافة السلام، دار ومكتبة الغد، مصر، 2009.
**عبد الوهاب المسيري: من المادية إلى الإنسانية الإسلامية، سلسلة أعلام الفكر والإصلاح في العالم الإسلامي، رقم 7، مركز الحضارة لتنمية الفكر الإسلامي، لبنان، الطبعة الأولى 2008.
**طارق البشري؛ القاضي.. المؤرخ.. المفكر.. وداعية الإصلاح، سلسلة أعلام الفكر والإصلاح في العالم الإسلامي، مركز الحضارة لتنمية الفكر الإسلامي، لبنان، الطبعة الأولى 2011.
رابعًا: تأليف بالاشتراك
**إيران – مصر: مقاربات مستقبلية، تحرير: توفيق شومان، مركز الحضارة لتنمية الفكر الإسلامي، بيروت، سلسلة الدراسات الإيرانية/ العربية، رقم 1، الطبعة الأولى، 2009.
**يوميات الثورة المصرية، (تحرير: أحمد عبد الحميد)، مركز الجزيرة للدراسات، قطر، 2011 .
**الحركات الإسلامية في الوطن العربي، (إشراف: الدكتور عبد الغني عماد)، مركز دراسات الوحدة العربية، بيروت، 2013.

**السعوديون الشيعة: الفكرة والإشكاليات، مركز صناعة الفكر، السعودية، 2015.
**المجتمع المدني السعودي ؛ الملامح.. والأدوار، مركز صناعة الفكر، السعودية، 2015.
**الليبرالية في السعودية (الفكرة، الممارسات، الرؤى المستقبلية)، مؤسسة الإنتشار العربي (لبنان)، مركز صناعة الفكر للدراسات والبحوث (السعودية)، الطبعة الاولى: 2013.
**الحوار مع الآخر.. المنطلقات والضوابط، وزارة الأوقاف والشئون الإسلامية، قطاع الشئون الثقافية، الكويت، (كتاب مجلة الوعي الإسلامي، الإصدار الرابع)، الكويت، 2006.
خامسًا: أعمال حققها
**ديوان أمير الشعراء أحمد شوقي (الشوقيات)، تحقيق، مكتبة الإيمان، مصر، مكتبة جزيرة الورد، مصر، 2007.
**ديوان الشاعر حافظ إبراهيم، (تحقيق)، مكتبة الإيمان، مصر، مكتبة جزيرة الورد، مصر، 2009.
سادسًا: أعمال أعدها للنشر أو حررها
اكتشف وأعاد نشر رواية: اعترافات حافظ نجيب: مغامرات جريئة مدهشة وقعت في نصف قرن للمغامر المصري حافظ نجيب، وهي الرواية التي اقتبس عنها المسلسل التلفزيوني المصري الشهير فارس بلا جواد. وقد قدم لها وألحق بها دراسة عن حياة مؤلفها .
**اعترافات حافظ نجيب: مغامرات جريئة مدهشة وقعت في نصف قرن (إعداد للنشر) .

الطبعة الأولى، 1996، دار الحسام، لبنان، مصر.
الطبعة الثانية، دار الانتشار العربي، بيروت، 2003.

**حرر (بالاشتراك) موسوعة اليهود واليهودية والصهيونية، 8 مجلدات، لمؤلفها المفكر العربي الإسلامي المرموق الدكتور عبد الوهاب المسيري، دار الشروق، مصر، 1998 .

**حرر (بالاشتراك) موسوعة اليهود واليهودية والصهيونية، لمؤلفها المفكر العربي الإسلامي المرموق الدكتور عبد الوهاب المسيري، نسخة ميسرة ومختصرة (مجلدان)، دار الشروق بمصر بالاشتراك مع مركز زايد للتنسيق والمتابعة بدولة الإمارات، 2004 .

**القمة الأمريكية السعودية الأولى: القمة السرية بين الملك عبد العزيز ابن سعود والرئيس روزفلت (البحيرات المرة، 1945)، (تقديم وتحرير ودراسة)، بقلم: الكولونيل: وليم إيدي (أول وزير أمريكي مفوض بالسعودية)، ترجمة: حسن الجزار، مكتبة بيروت، سلطنة عمان، شركة دلتا، مصر، 2008.

**دع القلق وابدأ الحياة، تأليف: ديل كارنيجي، إعداد وتقديم ودراسة، دار الحرم للتراث، مصر، 2009.

**كيف تكسب الأصدقاء وتؤثر في الناس، تأليف: ديل كارنيجي، إعداد وتقديم ودراسة، دار الحرم للتراث، مصر، 2009.

**تربية المرأة والحجاب (ردًا على قاسم أمين)، تأليف: محمد طلعت حرب (باشا)، إعداد وتقديم ودراسة، دار الغد للنشر، مصر، 2009.

**العمانيون فى بوروندي، رومونجيه نموذجًا، تأليف: سلطان بن محمد بن حمدان الشرجي، (تحرير وتقديم)، الناشر: مكتبة بيروت (سلطنة عمان)، 2022.

رابعًا، مؤلفات منشورة إليكترونيًا عبر منصات: كوبو بوك (كندا)، وأمازون كيندل وجوجل بلاي (أمريكا)

**جمال البنا: تسويق التنوير بلغة الإثارة والإعلان.

**مقالات عن الهولوكوست (رؤية إسلامية).

**عبد الوهاب المسيري: حياة وأفكار.

**عن التحالف المسيحي اليهودي.

**السيف العربي بين جماليات الفن وضرورات الحرب

**الحرية والثقافة لجون ديوي (تحرير ومراجعة)

**قراءة في كتاب الحرية والثقافة لجون ديوي.

**كتب قرأتها

**مختصر تاريخ التكنولوجيا العسكرية (وعلاقتها بالأمن القومي)

**الإنجلوفونية القادمة: الجذور والملامح

**التفكيكية: من الفلسفة إلى النقد الأدبي

**الديموغرافيا وصراع الهوية: مسلمو أوروبا نموذجاً

**حوار مع القيادي الإخواني الدكتور سيد عبد الستار المليجي

**حوار مع المستشار طارق البشري.

**هوية مصر الإسلامية: بحث عن الذات أم خوف من الآخر؟

**منافٍ لها تاريخ

**هيكل والإسلاميون

**الإسلاميون والدولة الحديثة.
**التصوف والفن من منظور فلسفة الدين
**الأفريقانية.
**مسلمو أوروبا: إعادة إنتاج المسألة اليهودية.
**أحمد شوقي: حياته وشعره.
**العلم والخرافة والسياسة: بين أوراق نيوتن ورسالة فاسكو دي جاما.
**هكذا ساهم العلم في بناء إسرائيل.
**لغة السيم (من جهود المعاصرين في دراسة اللغة السرية)
**اللوبي الصهيوني: محاولة للفهم.
**قراءة في كتاب: "دولة المنظمة السرية"، لحسن العلوي.
**سلسلة دراسات في دولة التنظيم السري:
– 1دولة التنظيم السري: ملاحظات تمهيدية
– 2تنظيم إرهابي سري اسمه الجمعية الفلسفية المصرية .
**العلمانية أصل الإرهاب والاستبداد الحديث (مختارات مترجمة).
**أحلام أكثر بؤساً من الواقع!: مقالاتي في جريدة "الحياة اللندنية(2014 - 1999) "
**الإسلاميون التقدميون: اليسار الإسلامي التونسي والثورة.
**العصر الجليدي القادم: من التقارير العلمية إلى استوديوهات هوليود.

**جسر لا يؤدي إلى مكان!، مقالاتي في صحيفة المستقبل (اللبنانية).(2014 – 2009)
** بين الدولة العميقة ودولة المنظمة السرية.
**ريحانة النفوس: في أصل الاعتقادات والطقوس، تأليف القس بنيامين شنيدر (1807 -1877)، تقديم وتحرير.
**داعش لايف ستايل ودراسات أخرى.
**فاتيكان جيت: الانتهاكات الجنسية في الكنيسة الكاثوليكية عبر العالم.
**سالم الرحال يتذكر: أفق الأسطورة ... حضيض المأساة.
**قراءة في تقرير صادر من معهد كونراد إديناور عن الدولة.
**قراءة في تقرير صادر من معهد كونراد إديناور عن الجاهزية للصراع.
**مقالاتي في جريدة البيان الإماراتية الجزء الأول مقالات السنوات 1998 – 2002.
**وثيقة أمن قومي معلنة، مقالات منشورة في موقع "مصر العربية."

** What has Islam given to Humankind?, Nick James (Editor), Prof Mohamed M. Hussein (Translator), 2017.

خامسًا، جوائز

**جائزة مؤسسة اقرأ الخيرية، مصر، المسابقة الثقافية للشباب لعام 1991، المركز الثالث في مجال الشعر.

**جائزة مؤسسة اقرأ الخيرية، مصر، المسابقة الثقافية للشباب لعام 1992، المركز الثاني في مجال المسرح عن نص ما زال مخطوطًا.

**جائزة أفضل قصيدة (المركز الثاني) من المجلس الأعلى للثقافة، مصر، 1999، عن قصيدة: "نقوش على قبر شهيدة."

**جائزة الإبداع العربي من: دائرة الثقافة والإعلام بإمارة الشارقة بدولة الإمارات العربية المتحدة في مجال المسرح (المركز الثاني) عام 2000، عن مسرحية عاصمة للبيع.

**جائزة أحمد فتحي عامر في مجال الشعر (المركز الثاني) من الهيئة العامة لقصور الثقافة، مصر، الدورة الأولى، 2003.

**جائزة أحمد فتحي عامر في مجال الرواية (المركز الثالث) من الهيئة العامة لقصور الثقافة، مصر، الدورة الثانية، 2004، عن رواية القاهرة، بيروت، باريس.

**جائزة أفضل قصيدة (المركز الثاني) من نادي جازان الأدبي بالمملكة العربية السعودية في المسابقة الثقافية لعام 1423هجرية، عن قصيدة: "بقصائدي ويقيني."

سادسًا، أعمال نقدية تناولت أعماله

" **ممدوح الشيخ وعماد أو صالح شعاعان من شمس شعر تشرق"، منشور في: "كتابة: رؤى وذات"، صافي ناز كاظم، الهيئة المصرية العامة للكتاب، مصر، 2003.

" **مقاربات نقدية في شعر ممدوح الشيخ"، تأليف الأساتذة: رمضان أبو غالية، صبري عبد الرحمن، أحمد

مرسال، سامح القدوسي، إصدارات نادي الأدب ببيت ثقافة قويسنا، مصر، 2004.
**رسالة ماجستير عن مسرحيته: "عاصمة للبيع" في: جامعة جنت البلجيكية، للمستشرقة البلجيكية ماريكي فان كرايسبليك، 2006. (قيد الترجمة)
القاهرة... بيروت... باريس... لممدوح الشيخ: عندما يحل "الفرنسي" محل "الأمريكي" رمزا للشر – لحوم بشر معلبة في رواية مثيرة... مسيسة دون ضجيج، خالد جلال، موقع ديوان العرب، ٨ يوليو ٢٠٠٦
**القاهرة.. بيروت.. باريس .. لممدوح الشيخ، لحم بشري طعامًا لحيوانات أليفة، محمد العشري، جريدة النهار اللبنانية، 25 يناير 2007.
" **القاهرة بيروت باريس" لممدوح الشيخ: سرد مختلف.. ..حدث مثير.. ..ورؤية جديدة للذات والآخر، علياء المالكي، موقع دنيا الوطن، 1 مارس 2007.
**تنامي صورة "المدينة" في روايات بيروت، عبد الرحيم العلام، دراسة، مجلة نزوى الفصلية، سلطنة عمان، عدد 77، يناير, 2014.
**بيروت في المرايا الروائيّة العربيّة المُتكسِّرة، دكتور نبيل سليمان، جريدة عمان، سلطنة عمان، 28 أكتوبر، 2020.
" **اليهود في الرواية المصرية.. الاندماج والقطيعة"، مصطفى بيومي، دار إنسان للنشر والتوزيع، مصر، 2022.
سابعًا، جرائد ومجلات ومواقع إليكترونية نشرت مقالاته ودراساته:
**دوريات داخل العالم العربي وخارجه :

جريدة المستقبل (اللبنانية)، جريدة البيان (الإماراتية)، جريدة عمان (العمانية)، جريدة الحياة (اللندنية)، مجلة المجلة (اللندنية)، مجلة الجديد (اللندنية)، جريدة العربي الجديد (اللندنية)، مجلة الكلمة (اللندنية)، جريدة الدستور (المصرية)، جريدة الوطن (المصرية)، جريدة الوفد (مصر)، مجلة المحجة (لبنان)، مجلة اتجاهات الأحداث (الإمارات)، مجلة آراء حول الخليج (السعودية)، مجلة كلية الملك خالد العسكرية (السعودية)، المجلة العربية (السعودية)، مجلة فكر وفن (السعودية)، مجلة الوعي الإسلامي (الكويت)، جريدة الفنون (الكويت)، جريدة الاتجاه الآخر (هولندا)، مجلة الشاهد (قبرص)، مجلة رسالة الجهاد (مالطا)، مجلة الرائد (ألمانيا).

مواقع إليكترونية نشرت مقالاته ودراساته:

**موقع ناشري (الكويت)، موقع إسلام أون لاين (قطر)، موقع مصر العربية (مصر)، موقع ذات مصر (مصر)، موقع إضاءات (مصر).

ثامنًا: مساهمات أخرى

" **دولة المنظمة السرية، فيلم وثائقي، (الفكرة والإعداد والمادة العلمية)، قناة الجزيرة الوثائقية، قطر، 2009.

**أعدَّ وقدَّم برنامج "المحفل"، قناة الحكمة (مصر)، مباشر، .(2011)

**أعدَّ وقدَّم برنامج "من قلب الكيان الصهيوني"، قناة الحكمة (مصر)، مباشر، .(2011)

**أعدَّ وقدَّم برنامج "ساعة من القاهرة"، قناة الاتجاه (العراق)، مباشر، 2011)، 2013.(

**أعدَّ وقدَّم برنامج "إسلاميون"، قناة فلسطين اليوم (لبنان)، مسجل، 2013) ، 2015.(
**قُدِمت ورقته الفكرية: "ماذا أعطى الإسلام للبشرية؟" في أول مؤتمرات "اللجنة العالمية لنصرة خاتم الأنبياء صلى الله عليه وسلم"، (لندن، نوفمبر 2002).
**مشرف على تحرير الصفحة الدينية بجريدة الدستور، مصر2005) ، 2008.(
**عرضت فرقة مسرح دبي الأهلي الإماراتية مسرحية: "مملكة للبيع"، (إعداد وإخراج: عبد الله صالح) المقتبسة عن مسرحيته: "عاصمة للبيع"، دبي، يوليو 2009 .
**شارك في العديد من المؤتمرات العلمية والثقافية في: مصر، لبنان، ليبيا، الإمارات، والعراق.
**شارك في عشرات البرامج التلفزيونية والإذاعية، الثقافية والسياسية في مختلف القنوات الفضائية المصرية والعربية.
الجنسية : مصري
للتواصل:

E.Mail: mmshikh@hotmail.com